SRINIVAS INSTITUTE OF MANAGEMENT STUDIES

Mangalore - 575001

Mobile Business Services with special reference to Financial Sector

Written by

Dr. P. S. Aithal

Srinivas Publishers

Mangalore – 575 001

India

Table of Contents

S. No.	Contents	Page No.
1	**List of Figures**	ix
2	**List of Tables**	x
3	**Chapter I : Introduction to Mobile Business and Mobile Banking** 1.1 Introduction 1.2 Features of Mobile Business 1.3 Mobile business Value Chain 1.4 Advantages of M-business over E-Business 1.5 Mobile Business Activities 1.6 Implications to Application and Service Providers 1.7 Mobile Banking 1.8 Mobile Banking Business Models 1.9 Mobile Banking Services 1.10 Technologies Behind Mobile Banking 1.11 Mobile Payment Methods 1.12 Security Issues in Mobile Banking 1.13 Cost Versus Security 1.14 Communications Security 1.15 Client Authentication 1.16 Additional Security Issues 1.17 Research Issues in this Study	01
4	**Chapter II : Review of Literature on Mobile Business Technology, Mobile Banking Services & Security** 2.1 Introduction 2.2 Mobile Communication Technology 2.3 Mobile Payment Technologies 2.4 Review of Literature on Online Banking 2.5 Significance of Mobile Business in Financial Sector 2.6 Services in Online Mobile Banking 2.7 Review on Security Issues on mobile banking Transactions 2.8 Review on mobile payment 2.9 Conclusion	37
5	**Chapter III : Research Objectives and Methodology** 3.1 Introduction 3.2 Problem Definition, Requirement Specification 3.3 Objectives of Present Study 3.4 Scope of the Study 3.5 Conceptual Study on Banker's Perspectives on Mobile Banking 3.6 Conceptual Study on Customers Perspective on Mobile Banking 3.7 Requirements to next-generation mobile payment systems 3.8 GSM AND GPRS Security Architecture	77

	3.9 Security Requirements 3.10 Biometrics Authentication 3.11 Conclusion	
6	**Chapter IV : Results and Discussion** 4.1 Introduction 4.2 Business Implications 4.2.1. Benefits of online mobile banking from Banks' Point of view 4.2.2. Business Perspective of Mobile banking - SWOT ANALYSIS 4. 2.3. Benefit from Customers Point of view 4.3 M-banking Models 4.3.1. Consumer Oriented New Model : 4.3.2 Analysis of the model: 4.4 Secure SMS Solution Using new model through Biometric Authentication 4.4.1. Secure SMS Protocol 4.4.2 Security of the Secure SMS Protocol for new Model 4.5 Secure GPRS Solution for new model through Biometric Authentication 4.5.1 Extension of present WAP implementations 4.5.2 New Secure GPRS protocol 4.5.3 Security of the Secure GPRS Protocol 4.6. Conclusion	106
7	**Chapter V : Summary and Conclusions** 5.1 Introduction 5.2 Summary of the Project 5.3 Recommendation to the Customers 5.4 General Conclusion 5.5 Limitations and Scope for Further Work	132
8	**Bibliography**	140
9	**List of Publications**	149

List of Figures

Figure No.	Figure Name	Page No.
Fig. 1.1	SMS Network Architecture	21
Fig. 1.2	WAP Network Architecture for Mobile Applications	21
Fig. 2.1	Wireless network technology evolution	39
Fig. 2.2	From 2G to 3G in three dimensions: the 3G service space	41
Fig. 2.3	Technological threat and opportunity assessment	45
Fig. 2.4	Growth of worldwide mobile phone sales, number of subscribers etc on a yearly basis	48
Fig. 3.1	Modified customer equity approach model	83
Fig. 3.2	Technology Acceptance Model : Theory of Customer Stimulation by Education and Training for Usage (TCSET)	85
Fig. 3.3	TCSET Model applied to Online Mobile Banking	88
Fig. 3.4	GSM Architecture	94
Fig. 3.5	WAP Protocol Suite Source	97
Fig. 3.6	Biometric authentication system	101
Fig. 4.1	Benefits of mobile banking from bank's point of view	107
Fig. 4.2	Consumer oriented model - uses Private Network Service Provider for enhanced security.	116
Fig. 4.3	The Structure of a Secure SMS Message	123
Fig. 4.4	Structure of message sent	128

List of Tables

Table No.	Table Title	Page No.
Table 1.1	Mobile Business Value Chain	09
Table 1.2	Classification of mobile banking Services	19
Table 2.1	Push or Alert and Pull or Request Facilities available in Indian Banks	60
Table 2.2	Threats and Vulnerabilities Associated with the Access Device	73
Table 2.3	Threats and Vulnerabilities Associated with Transactions	73
Table 2.4	Threats and Vulnerabilities Associated with Other Interactions	74
Table 2.5	Threats and Vulnerabilities Associated with Mobile Infrastructure	75
Table 3.1	Main characteristics of biometric technologies.	105

Chapter I

Introduction

1.1 Introduction to Mobile Business

The convergence of wireless devices and the Internet is creating an important new channel to business and the next wave of change across industries. Mobile business (or M-business) will enable organizations in every industry to expand their markets, improve their services and reduce their costs. M-business can best be described as the transaction of data between mobile devices. The most significant factor driving M-business is undoubtedly the proliferation of mobile telephones, wireless-enabled personal digital assistants (PDAs) and other devices that enable users to conduct transactions anywhere at any time.

Mobile phones have become an integral part of the 21st century landscape with an expected penetration of 4.5 billion by 2011. While North America and Europe have the highest penetration rates, reaching 100%, in many Western countries, South America and Asia represent the fastest growing mobile markets. The mobile phone is the one device that people carry with them at all times. Services beyond voice and text messaging are booming all over the globe and users want the same services on their mobile phone that they can get through an Internet connected PC. Mobile phones represent a cost-effective solution for bank and unbanked users, financial institutions and operators, allowing them to bridge the digital divide in places where traditional banking and Internet services are too expensive or simply nonexistent.

Mobile Banking helps the customer's anytime access to their banks. Customer's could check out their account details, get their bank statements, perform transactions like transferring money to other accounts and pay their bills sitting in the comfort of their homes and offices [1]. Much of the discussion surrounding M-business has been narrowly focused on m-commerce, a subset of M-business that involves the use of mobile devices for marketing, selling and buying products and services over the Internet, "third generation" (3G) networks, or other supporting technologies. But it is believed that M-business is a far greater one that will build on organizations' e-business transformations and capabilities and provide the backdrop for a further qualitative shift in business operations. M-business will comprise a broad spectrum of applications, from communication and entertainment to consumer transactions and corporate services. These services will not be limited to one particular type of relationship, like business-to-consumer (B2C), but also will include business-to-business (B2B), business-to-employee (B2E), consumer-to-consumer and device-to-device relationships. For this reason, M-business has been dubbed A-A business : anytime, anywhere.

M-business is not just e-business without fixed connections, but it is an entirely new way of designing and deploying a wide range of systems and solutions that are :

- Personal.
- Convenient.
- Easy to use.
- Always available.
- Accessible in real time.
- Location sensitive.

The biggest risk for organizations is believing that M-business opportunities are far years away. The pace with which businesses accept emerging technologies is accelerating. M-business is here today, and growing at a tremendous rate [2].

Analysts predict that in the next five years the penetration of mobile devices will outpace that of televisions — and the more users have such devices, the more services they will demand. But behind the scenes, there are other drivers moving this revolution forward, which include :

- **Advancements in network technologies -** Mobile-network operators around the world are investing large sums of money in licenses and in building a new generation of networks. Network technologies that can support always-on connectivity will allow users to immediately send and receive voice and data services. At the same time, business investment is continuing apace in innovation at other levels of the network. Device manufacturers are creating prototypes of the products that might exist in the near future, and the race is on to create new standards for operating platforms.
- **Falling costs for airtime and wireless devices -** The cost of mobile devices and basic services such as voice and short messaging service (SMS) has plummeted. No longer is the mobile device a status symbol. It is becoming an intrinsic part of everyday life for millions of people.
- **The ability to link elements in different value chains, in real time, to provide a dynamic, personalized service -** Businesses those link services, many of which already exist independently, will streamline their customers' transactions. For example, linking aeroplane ticket purchases, car rental bookings and hotel reservations, then communicating all the information via messaging to mobile devices, would make travel planning easier. In order to offer these new services, businesses are beginning to enter into new alliances and partnerships, both within and outside their industries. This process in itself creates new possibilities and new business opportunities. M-business raises

critical questions about strategic adaptation for every organization. It will herald the emergence of entirely new value chains and business models, not to mention new levels of personalized service. It will lead to new business alliances and a wave of convergence between industries. At a fundamental level, it will enable organizations to dynamically reconfigure their value chains and develop new relationships with employees, suppliers, customers and competitors.

- **The ability to tailor services for end-users' various needs** — Taking one-to-one marketing to a higher level — will become a new source of competitive advantage. By changing the nature of communication and interaction, customer relationship management will take on a new dimension. M-business will also facilitate efficiency gains through workforce management. Mobile technologies offer the potential for tasks to be scheduled for the right worker, with the right set of tools, at the right location and at the right time. They also increase the likelihood that customer enquiries can be resolved on the first port of call.

Organizations that succeed at M-business will have to do more than simply place supply chain management systems onto mobile devices, or mobile-enable enterprise resource planning (ERP) solutions. They will have to capture business "events" and translate them in real time into whatever format is required. Transaction volumes will be high, and the required service levels will far exceed those delivered by today's technology solutions. M-business is set to make a major difference in all aspects of operations and management, and it opens up a whole avenue of major top-line revenue growth opportunities and bottom-line productivity gains for organizations in all industries. Organizations need to examine where their prospects for efficiency gains and improvements to customer service. This means anticipating changes in all areas of their value chains, which include : Administration, Human resources, Research and development, Production, Purchasing and sourcing, Sales and marketing, Distribution and logistics.

In this introductory Chapter, an overview of opportunities and challenges for mobile business is given. This includes various value propositions, implications of mobile devices, implications of mobile networks, mobile business value chain, advantages of mobile business over e-business, mobile business activity including value added applications, legal concerns and implications to applications and service providers. The chapter also contains information about mobile banking models, services, technologies, payment methods, and securities of financial transactions.

1. 2. Features of Mobile Business

1.2.1. Value Propositions for M-business

Value propositions define the relationship between supplier offerings and consumer purchases by identifying how the supplier fulfills the customer's needs across different consumer roles [3]. Specifically, it defines the interdependence between the performance attributes of a product or service and the fulfillment of needs. The value proposition furthermore solidifies the relationship between the customer and various dimensions of product value. Thus, customer satisfaction is merely a response to the value proposition offered by a specific product/service bundle. For e-business, the establishment of a value proposition is rudimentary to any consumer-oriented strategy creation.

The mobility afforded wireless devices shapes M-business into a disparate entity from conventional e-business. Consequently, value propositions are likely to be new, different and novel for mobile e-business. The primary advantage of mobile devices is to provide a superior offering of value-for-time to users. That is, by accessing the Internet/SMS through mobile devices, users will be able to realize additional value allowances for any specified period of time, which fixed-line users will not be able to achieve. Information may now truly become available anytime, anyplace and on any wireless device. As such, value propositions of e-business will be forced to change to reflect the underlying dimensions of value-for-time for users. Specifically, M-business differs from e-business on the following value proposition attributes:

1. Ubiquity : Mobile devices offer users the ability to receive information and perform transactions from virtually any location on a real-time basis. M-business users will have a presence everywhere, or in many places simultaneously, with a similar level of access available through fixed-line technology. Communication can take place independent of the user’s location. The advantages presented from the omnipresence of information and continual access to commerce will be exceptionally important to time-critical applications. Mobile businesses, for example, can leverage this value proposition by providing alert notifications, such as for auctions, betting, and stock price changes, which are specified by the user as an important part of relevant personal content. As such, the real-time, everywhere presence of M-business will offer capabilities uniquely beneficial to users. Industries that are time and location sensitive, such as financial services and travel, are likely to benefit from businesses exploiting this value-added feature of mobile business.

2. Convenience : The ability and accessibility provided from wireless devices will further allow M-business to differentiate its abilities from e-business. People will no longer be constrained by time or place in accessing e-business activities. Rather, M-business could be accessed in a manner which may eliminate some of the labor of life's activities. For example, consumers waiting in line or stuck in traffic will be able to pursue favorite Internet/SMS based activities or handle daily transactions through M-business applications. Consumers may recognize a special comfort which could translate into an improved quality of life. One opportunity to increase value lies in M-business capabilities that allow consumers to shop at where they are not located. This ability to obtain information and conduct transactions from any location is inherently valuable to consumers. As such, M-business offers tremendous opportunities to expand a client-base by providing value-added services to customers. By making services more convenient, the customer may actually become more loyal. Consequently, communication facilities within M-business are key applications for the delivery of convenience. Consumers will be looking for M-business applications which can deliver functions like : sending and receiving e-mail, voice mail forwarding, conference calling, faxing, document sharing, instant messaging; as well as transactional based activities.

3. Localization : Knowing the location of the Internet/mobile user creates a significant advantage for M-business over wired e-business. Location-based marketing, via global positioning technology, will soon be available in all mobile devices. Through GPS technology, service providers can accurately identify the location of the user. Utilizing this technology, M-business providers will be better able to receive and send information relative to a specific location. Since mobile devices like cell phones are almost always on, vendors will know the location of their customers and can deliver promotions based upon the likely consumer demands for that location. Location-specific information leverages the key value proposition of M-business over traditional e-business by supplying information relevant to the current geographic position of the user. M-business providers will be able to both push and access information relevant to the user’s specific location. Mobile web-sites may serve as points of consolidation of consumer information and disseminate the relevant information for a particular location based on profile data built on the user's past behavior, situation, profile and location. As such, real time discounting may become the "killer application" for M-business.

4. Personalization : Mobile devices are typically used by a sole individual, making them ideal for individual-based target marketing. Mobile offers the opportunity to personalize messages to various segments, based upon time and location, by altering both sight and sound. New developments in information technology and data-mining make tailoring messages to individual consumers practical and cost-effective. For example, upon employing mobile Internet device, advertising messages tailored to ones individual preferences can be provided. Relevance of material and the "de-massing" of marketing becomes possible through the personal ownership of mobile devices.

5. Conditions of Usage : The mobile user may be engaged into another activity, like traveling, meeting people, etc., rather than sitting in front of his/her desk top terminal.

6. Adaptability : Mobile business applications should be adapted to the environment of their clients. Adaptability is possible along various dimensions including the type of the device in use, the currently available communication bandwidth as well as location and time.

7. Broadcasting : Some wireless infrastructures, such as cellular architectures and satellite networks, support broadcasting (i.e., simultaneous delivery) of data to all mobile users inside a specific geographical region. Broadcasting offers an efficient means to disseminate information to a large consumer population. This mode of operation can be used to deliver information of common interest to many users such as stock prices, weather information or for advertising.

A value proposition is developed as superior consumer value is created through an increasingly targeted Internet experience for mobile users. For M-business, the technological limitations magnify these value-for-time propositions. It has been estimated that every additional click-through, which a user needs to make in navigating through a commercial online environment with a mobile device, reduces the possibility of a transaction by 50 per cent [4]. Providing the user with the desired, most relevant information without forcing a complex click-through sequence will significantly improve the effectiveness of any mobile e-business strategy. Value-for time propositions become maximized for those business strategies best able to implement M-business's distinguishing capabilities. M-businesses will become differentiated from traditional e-business based upon their abilities to integrate and actuate the advantages to the mobile devices. Various applications may provide differing value for mobile Internet users.

1.2.2. Implications of the Mobile Devices

Mobile devices that are of interest to mobile communication can be divided into four categories based on their processor, memory and battery capacity, application capabilities (SMS, WAP, Web, I-mode), as well as physical size and weight. These categories are (from weakest to strongest) : usual voice handsets with SMS capability, WAP phones, communicators/PDA with wireless communication capability, and laptops with wireless communication facilities. To be easily carried around, mobile devices must be physically light and small. The smaller and lighter the devices are, the *more portable* they are. In addition, a mobile device should be a multipurpose device (voice phone, data transmitter, PDA, etc.) so that the user does not need to carry too many gadgets. Portability considerations, in conjunction with a given cost and level of technology, will keep mobile elements having less resources than static elements. The devices have small screens and small multifunction keypads; the former fact necessitates the development of appropriate visual user interfaces, different from the PC or laptop. They have comparably less memory, disk capacity and computational power than traditional computing devices. Portable devices rely for their operation on the finite energy provided by batteries. Even with advances in battery technology, this energy concern will not cease to exist. This is because the conserved energy depends primarily on the weight, volume of the battery. There are higher risks to data stored and transactions performed in mobile devices, since it is easier for mobile devices to be accidentally damaged, stolen, or lost than fixed devices.

1.2.3. Implications of the Wireless Networks

The necessary networking infrastructure for wireless mobile computing in general combines various wireless networks including cellular, wireless LAN, private and public radio, satellite services, and paging [5]. As compared with wire-line networks, wireless communications add new challenges:

C-autonomy : The handsets in the wireless radio networks are normally not always communicating with the network infrastructure, i.e., they are unreachable. There are numerous reasons for this behavior that can be described under C(ommunication)-autonomy [6]. First, disconnections may be voluntary, e.g., when the user deliberately avoids network access during nighttime, or while in a meeting, or in other places where the user does not want to be disturbed. In cases that the handset does not have voice capabilities, and thus disturbing is not a big issue, it is still often reasonable to cut the wireless communications with the network to reduce cost, power consumption, or bandwidth use. The break in on-going communication or incapability to set up any communication can also happen against the will of the user, e.g., when a user enters a physical area where there is not any or not enough field strength for a successful communication battery becomes suddenly empty, or hand-over between base stations does not succeed and the connection is therefore lost.

Bandwidth restrictions and Network topology : In the case of many wireless networks, such as in cellular or satellite networks, communication channels have much less transfer capacity than wire-line networks. This is caused by the fact that the used modulation and channel allocation schemes designed for voice traffic have rather modest upper bounds. Further, wireless communications are much more error prone than wire-line communications and require much redundancy in the channel coding of the payload.

Asymmetric communications : Some wireless networks offer asymmetric transfer capacity for up- and downlink. The asymmetric transfer capacity on uplink and downlink can be applied in a reasonable way if the network offers broadcast facility. This is unfortunately not a strong side of the telecom networks, because they were designed for connection-oriented point-to-point communications. Wireless LANs are better in this respect, because they apply packet broadcast protocols. GSM networks have broadcast facility on the control channels, but the amount of application data that can be transferred on them is small. The currently very popular short messages (max 160 characters) are an example of such data that is transferred over control channels. If used, e.g., to broadcast multimedia contents over the network, the network would collapse, because controlling the traffic would not be possible any more. Still, the asymmetric transfer capacity is an important asset in cases where the wireless client usually sends a short request and gets a large data set as a response.

***Variant bandwidth and bursty traffic* :** Currently, multi-network terminals are emerging that can use several networks to communicate. Typical forerunners are the dual-band devices that are able to use 900 MHz and 1.8 GHz GSM networks. New products are emerging to the market that are able to also use WLANs and possibly Bluetooth, together with GSM, GPRS, and soon also UMTS network infrastructure. Wireless technologies vary on the degree of bandwidth and reliability they provide. In this respect one can speak of variable bandwidth. Another phenomenon also observable in the wireless world is bursty traffic which is the case with Internet-type networks and this holds in different time scales.

Variant tariffs : For some networks (e.g., in cellular telephones), network access is charged per connection-time, while for others (e.g., in packet radio), it is charged per message (packet). In the WAP environment there is a larger variety of tariffs, e.g., session-based, transaction-based, connection time-based, while in mobile e-commerce the range of tariffs is even wider.

Mobility : GSM infrastructure allows roaming all over the world, i.e., the user can get access to voice and data services basically in any other GSM network. Mobility causes diverse phenomena. The available bandwidth might vary, for instance, a mobile terminal may rely on low-bandwidth networks outdoor, while inside a building it may be offered reliable high-bandwidth connectivity or even operate connected via wire-line connections. Moreover, there may be areas with no adequate coverage resulting in disconnections while on the move. There may be also variability in the provision of specific services, such as in the type of available printers or local weather reports. Furthermore, the services offered by the telecom network used might differ from those at home. This might have drastic consequences for mobile business, if the e-commerce infrastructure used needs them. Finally, the resources available to a mobile element vary, for example, a docked computer or PDA has more memory or is equipped with a larger screen. Mobility also raises very important security and authentication issues.

1.3. Mobile business Value Chain

As described by Barnett et al., [7], transport, basic enabling service, transaction support, presentation service, personalization support, user application, and content aggregators are the seven links in the mobile business value chain (illustrated in Table 1.1).

Table 1.1 : Mobile Business Value Chain

	Link Name	Function
1	Transport	To maintain and operate the infrastructure and equipment to guarantee data communication between mobile users and application providers.
2	Basic enabling service	To provide services such as server hosting, data backup, and system integration.
3	Transaction support	To provide the mechanism for assisting transactions, for security, and for billing users.
4	Presentation service	To convert the content of Internet-based applications to a wireless standard suitable for the screens of mobile devices.
5	Personalization support	To gather users' personal information, which enables personalized applications for individual users.
6	Content aggregators	To provide information in a category or search facilities to help users find their way around the Internet.
7	User applications	To carry out mobile commerce transactions for Mobile consumers.

From the perspective of a transaction, the following entities are the main participants in mobile business:

1. Customer. He or she can initiate a transaction in one place, receive the service in another place, and complete the transaction in a third place. The places can be in different cities, states, and countries.

2. Content provider. It provides customers specific content, which can be transmitted through a WAP Gateway or through a portal.

3. Mobile portal. Different from an Internet portal, it offers customers services with a greater degree of personalization and localization.

4. Mobile network provider. It plays different roles in mobile business varying from a simple mobile network provider to an intermediary, portal or trusted third party, depending on where it stands in the mobile business chain.

1.4. Advantages of M-business over E-Business

E-business has conquered the world. Despite the bursting of the dotcom bubble, it is hard to believe today how one managed to transact any business in the early 1990s without the Internet. Whether employed for information, support or advertising, nearly every business in the world of any size has a website. E-business has revolutionized how many companies do business, allowing for new business models and spawning completely new types of businesses. So with e-business less than 10 years old, is the world ready for something new, something with a potential of revolutionizing business practices the way e-business did? The answer is “Yes.”

Like e-business that preceded it, M-business as a transformational force is here to stay. In the next few years, mobile business or M-business will emerge as a powerful new approach for conducting business. It will become as pervasive by 2008 as e-business had become by the late 1990s. While the transformation induced by M-business would be dramatic, it would not necessarily replace e-business. M-business would enhance existing e-business functions and applications and launch new ones, totally mobile instead of being tied to desktop terminals. In many ways, M-business would establish new patterns of doing electronic transactions, over and beyond what fixed-line e-business is capable of.

E-business happened because of the combined efforts of the personal computer, telecommunications, software, and office technology industries. M-business, similarly, is happening because of the combined efforts of the world’s mobile handset manufacturing, telecommunications, computers, software, and office technology industries. In this massive global business, M-business is appearing as a new platform for creating product and service differentiation. Internet and e-business helped drive the supply and demand for multimedia computers. The underlying chip and display technology are upgrading at tremendous speed and as the mobile business matures, it would transform the handset – rendering it as different from its predecessors as today’s desktop PC screen is from the green-tinted, non-graphic PC screen of the early 1980s.

The variables that are likely to set M-business apart from e-business are as follows :

User Experience

The biggest differentiator between e-business and M-business is the sensory experience of the user. In e-business, the user is in a stationary position in front of a PC terminal, and interfaces the content using a keyboard and point-and-click devices. In M-business, this is replaced by total mobility and the terminal can be voice or touch activated.

Different Terminals

A disposable terminal is probably the most radical way of describing how different terminals could be. Today’s manufacturing technology aided by the unrelenting progress of Moore’s law will allow an ever-increasing differentiation of terminal offerings. Terminals that are bendable, so that they can be rolled up, have been demonstrated at trade shows. Miniature sized terminals allow for packaging into ever-changing shapes and forms. Pre-paid phone service is just the introduction to other pre-paid services, complete with ‘free’ terminals. Multimedia is here to stay and will continue to evolve.

Multi-Transaction Services

M-business services could be scheduled and delivered in multiple ways. Users can choose to have a variety of services delivered at the times and places that they specify. In some cases, the services can be pre-scheduled (for peak hours, late night, birthdays, etc.). In still other cases, the network and the device can make intelligent assessments of what services are needed and proffer such services.

Integration with Enterprise Applications

With M-business, a business enterprise could move most of its capabilities out into the field. Services and applications that required office visits and meetings could now be delivered while moving with full access to all enterprise applications residing on business IT and information systems.

Field Third Party Applications

Terminals that are M-business ready can receive services not just from the primary wireless service providers but also from a variety of third-party providers. Most of these third-party providers would work through the wireless service operators. In some cases, the terminal may be able to communicate directly to third-party wireless service providers, through ad-hoc information exchange set ups or direct connectivity. The source of applications and information therefore becomes transparent to the user.

Geographic Positioning

From a continent to the corner of a street, M-business networks would be able to locate the user and tailor the service mix to the geographical location, keeping in view the constraints and opportunities of the geographical setting as well as the preferences of the user. A service would therefore work differently in India than in Honk Kong, London or New York based on profiles or regional preferences.

Mobile Flexible Configurations

Today’s user profiles – whether in e-business or M-business settings – show the way to flexible configurations. But rather than requiring manual setups and changes, the m-services of the future will be automatically configured. So the minute a user leaves the home area, the service will be automatically configured with ring-tones, forwarding information and even downloaded information as the user travels. If the user wants to configure it in a new way, a simple code will download a new configuration.

Integration with Mobile Services

New M-business services would be easy to integrate with preexisting mobile services. For example, M-business offerings could easily incorporate a variety of existing messaging services, SMS and e-mail. They could also use conference bridges, network based calling, voice mail as well as many emerging services like downloadable hand-set applications, Multi-Media Messaging and information services.

Mobile Flexible Services

With easier integration of services, users would be able to avail of pre-packaged as well as programmable service-mixes. Some M-business systems would offer a service bundle from which the users would be able to choose and blend a variety of services.

Flexible Location

With M-business, the user can work, do daily chores, and/or play at work, home, recreational, shopping, and vehicular locations. The coming blurring of roles in the era of M-business will spawn multiple opportunities as well as trigger major social changes.

Network-enabled M-business Services

Extrapolating existing business approaches and paradigms into new areas is the most obvious way of looking into the future. For M-business, the problem with this approach – treating M-business as a simple extrapolation of e-business – is that it fails to take into account the dramatic differences (as well as different capabilities) between the two. Some of the most dramatic differences are screen size and the mobile user experience. But equally important are the fact that M-business services will be built (assembled) from different ‘piece-parts’ than e-Business. Wireless service operators will deliver some of these ‘new’ piece-parts and many of these are being discussed and implemented today. Examples include location information Application Programming Interfaces (APIs) and services. Certainly in future, there will be other, as-yet-unknown service piece-parts.

Basic Data Transport Services

At the most basic level, adding data transport capabilities to simple mobile voice telephony opens up some opportunities for M-business. The evolution of Web-browsing from today’s slow WAP speeds to higher data rates will revitalize some of this market. Pure data transport to support custom terminal based network applications, like those used by today’s package delivery services, will continue to grow as enterprises start to capitalize on higher speed data transport to develop new business productivity and enhancement applications.

Additional Network Services

Enhancing basic mobile data access and web-browsing capabilities with additional network services and specialized terminals add more value to the M-business concept. Examples of this include the handheld device, which provided mobile email and messaging capabilities. Present day technology provides GPS capabilities in the mobile phone, making it a useful device for navigating in cities as well as in wilderness. Multi-media messaging is certainly positioning itself as a major value added service, replacing today’s SMS as a key data service. Some network data services will utilize location information, for example delivering messages only in certain areas.

APIs for Network Services

APIs for network services allow for tighter service integration of Messaging, Location Based Services, Usage monitoring, and Billing. These API’s are intended to be used by third parties or business enterprise applications to offer services that are more closely integrated with network services, utilize network billing or deliver services that are based on where the user is located.

Additional Services

As an additional value-adding step, the wireless operator can offer additional M-business oriented services providing complete value added information, tracking, billing or messaging services. These complete service packages can be utilized by business customers in order to develop more complete applications for their users.

Complete Integrated Service Packages

As an ultimate value-adding step, the M-business service provider can design and offer fully integrated service packages that solve complete problems.

1. 5. Mobile Business Activities

The essence of mobile business revolves around the idea of reaching customers, suppliers, and employees regardless of where they are located. It is about delivering the right information to the right place at the right time. This flexibility of mobile business is made possible by the convergence of the Internet, enterprise applications, and wireless technology [8](Clarke, 2001). Mobile business, enabling information exchange and purchases using mobile devices, provide different things to different people: to customers, it represents convenience; merchants associate it with a huge earning potential; and service providers view it as a large unexplored market. Japan and Europe are already witnessing early successes in mobile business. In Japan, NTT DoCoMo's iMode phone has emerged as a great success highlighting the application of wireless technology to a business environment. Introduced in February 1999, NTT DoCoMo iMode provides a continuous Internet connection via mobile phones, and connects users to a wide range of online services, many of which are interactive. All services link directly to the iMode portal Web site, and users can access any service virtually instantly by pressing the mobile phone's dedicated iMode button, iMode has already attracted more than 13 million Japanese consumers, particularly youth. Connected continuously to the Internet, these 13 million users can send e-mail, get stock quotes, and play online games. Soon they will be able to use on-line map guides and even conduct commercial activities by phone. Europe has also embraced a simple mobile data service whole-heartedly. Short Message Service (SMS) technology makes wireless e-mail a reality, and the new Wireless Application Protocol (WAP) facilitates Web browsing and other Web-based transactions on mobile phones. Bluetooth, another European data initiative, further establishes a common standard for a wide range of appliances and industrial devices to communicate wirelessly. With new developments in technology, it is estimated that more than half of the European mobile business market in the next few years will include financial, advertising, and shopping services [9].

1.5.1. Value-Added Applications

As mobile business extends the current Internet sales channel into the more immediate and personalized mobile environment, it also revolutionizes the business world by presenting it tremendous opportunities to provide additional value to hard-to-reach end customers [10]. These value-added services include:

1. Easy, timely access to information (e.g., the latest availability of flights) : Delivering a service that not only reaches more people but also is available all of the time, mobile business enables consumers to make purchases from wherever they are, whenever they are ready. This will result in an increase in revenue to the company providing the mobile services.
2. Immediate purchase opportunity (e.g., last minute purchases of tickets or gifts) : Provided with a personalized, immediate opportunity to purchase, the customer will make the purchasing decision on the spot and not go to an alternate source.
3. Wireless coupon based on user profiles : Since a mobile device's location can be determined precisely, the stores around the mobile device user can transmit user-specific information, such as current sales or specials, and alert the user about similar upcoming events. Wireless coupons, which enable an advertiser to deliver a geographically targeted and time-sensitive message to a willing consumer directly with a promotional offer virtually anytime and anywhere, will increase acquisition efficiency and allow direct offers suited to user profiles or stated user's preferences.
4. Beaming money : Some bank transactions such as withdrawals and deposits will be conducted via mobile terminals in the near future. Electronic money can even be transferred to mobile devices allowing the latter to be used for electronic payments.
5. Buddy finding : This location technology will quickly alert a user when his or her friend or colleague is nearby. It will also help the user to locate the nearest restaurant or ATM.

The only limit on the number and types of mobile business applications is our imagination. [11] identified a few important classes of applications such as mobile finance applications, mobile advertising, mobile inventory management, and product location shopping. As wireless technology further evolves, its application in business will only be broadened by more and more innovative mobile business possibilities.

1.5.2. Legal Concerns

Apart from its technical and business obstacles, the implementation of mobile business has its legal concerns too. The application of traditional law to the mobile Internet is not always a straightforward process. Legal issues plaguing mobile business are similar to those facing e-business. Some of them are how to maintain privacy, how to deal with defamation, how to protect intellectual property, and how to treat Internet taxation [12]. Like the wired Internet, the wireless Internet also poses significant challenges to our legal structure.

1.6. Implications to Application and Service Providers

The prospect and advantages of mobile business may appear obvious to many of us, but the path to success using mobile business is not necessarily so plain. Technical restrictions of mobile devices and wireless communication, business concerns, and legal constraints complicate the practical use of mobile business. The obstacles confronted by mobile business applications and service providers, and the solutions available to some of the problems are given below :

1. Changes in business strategies : To stay competitive and realize genuine productivity benefits from mobile business, many organizations actually need to be redesigned. They will have to make fundamental changes in organizational behavior, develop new business models, and eliminate the inefficiencies of the old organizational structures. The process of rethinking and redesigning is a demanding task.

2. Investment risk : A major problem faced by mobile business is the huge investment required to implement and operate it. Engineering massive organizational and system changes to reposition the organization strategically is complicated as well as expensive. How can organizations obtain a payoff from their investment in wireless technology? Understanding the costs and benefits of mobile business is difficult.

3. Customer confidence : Customers need to be assured that their financial information is secure, and that wireless transactions are safe. The mobile business service should improve its reliability and stability by providing comprehensive technical and operational support to give users positive experiences and increase their satisfaction, and thus enhance the service provider's reputation and build customers' loyalty.

4. Simplicity in use : Many who try mobile business are frustrated and stop using it after a few attempts. Users need a simple experience, directly relevant to their mobile needs, and to enjoy the benefits of immediacy. Simplicity in use is critical to a successful mobile service.

1.7. Mobile Banking

The advent of mobile communication technology innovations and globalization are increasingly driving the financial services to become ubiquitous, personalized, convenience, disseminative and secured. The lack of security and a high level of fraud is seen as a major obstacle to people embracing the possibilities and advantages of using internet based online banking services. For online financial transactions, the security at both the client and the server end must be taken care. On the client side, the poor platform integrity, the multitude of default CA certificates and the arcane user interface pose severe security threats. On server side, most important types of system attacks which pose severe threat on internet financial transactions are : Password cracking, screen emulators, data diddling, social engineering, malicious code, distributed denial of service, physical perimeter penetration, and wireless intercepts. Online banking through mobile service providers is more secure than online banking through internet because of the usage of private network of the service provider and the user's personal mobile device.

In mobile banking applications, the primary concern is the limited size and poor user interface of mobile devices than the security due to the fact that the characteristics of mobile architectures are strictly controlled can make it easier to obtain satisfactory security. Communication security is often described in terms of confidentiality, integrity, authentication and non-repudiation of transmitted data. These security services are in turn implemented by various mechanisms that are usually cryptographic in nature. In addition there is confidentiality of traffic, of location and of the communicating parties' address, all of which are important for privacy. A casual level of security is usually provided implicitly even without taking any extra measures. Casual authentication between mobile phone users is indirectly provided by the calling and called party numbers. Confidentiality of transmitted data can be provided by encrypting the information flow between the communicating parties, and the encryption can take place end-to end between the communicating parties or alternatively on separate legs in the communication path. Mechanisms for implementing confidentiality of traffic, location and addresses will depend on the technology used in a particular mobile network. Different parties will have different interests regarding authentication and non-repudiation services. Network operators are interested in authenticating the users for billing purposes and to avoid fraud. This kind of authentication also helps secured mobile banking through such networks. Users and banking service providers are interested in authenticating each other and might also be interested in authenticating the network service provider.

1.8 Mobile Banking Business Models :

A wide spectrum of Mobile/branchless banking models is evolving. These models differ primarily on the question that who will establish the relationship (account opening, deposit taking, lending etc.) with the end customer, the Bank or the Non- Bank/Telecommunication Company (Telco). Models of branchless banking can be classified into three broad categories - Bank Focused, Bank-Led and Non Bank-Led.

Bank-focused model

The bank-focused model emerges when a traditional bank uses non-traditional low cost delivery channels to provide banking services to its existing customers. Examples range from use of automatic teller machines (ATMs) to internet banking or mobile phone banking to provide certain limited banking services to banks' customers. This model is additive in nature and may be seen as a modest extension of conventional branch-based banking.

Bank-led model

The bank-led model offers a distinct alternative to conventional branch-based banking in that customer conducts financial transactions at a whole range of retail agents (or through mobile phone) instead of at bank branches or through bank employees. This model promises the potential to substantially increase the financial services outreach by using a different delivery channel (retailers/ mobile phones), a different trade partner (Telco / Chain Store) having experience and target market distinct from traditional banks, and may be significantly cheaper than the bank based alternatives. The bank-led model may be implemented by either using correspondent arrangements or by creating a JV between Bank and Telco/non-bank. In this model customer account relationship rests with the bank.

Non Bank-led model

The non-bank-led model is where a bank does not come into the picture (except possibly as a safe-keeper of surplus funds) and the non-bank (e.g. Telco) performs all the functions.

1.9 Mobile Banking Services :

Banks offering mobile access are mostly supporting some or all of the following services [13]:

Account Information

- Mini-statements and checking of account history
- Alerts on account activity or passing of set thresholds
- Monitoring of term deposits
- Access to loan statements
- Access to card statements
- Mutual funds / equity statements
- Insurance policy management

- Pension plan management

Payments & Transfers

- Domestic and international fund transfers
- Micro-payment handling
- Mobile recharging
- Commercial payment processing
- Bill payment processing

Investments

- Portfolio management services
- Real-time stock quotes
- Personalized alerts and notifications on security prices

Support

- Status of requests for credit, including mortgage approval, and insurance coverage
- Check (cheque) book and card requests
- Exchange of data messages and email, including complaint submission and tracking

Content Services

- General information such as weather updates, news
- Loyalty-related offers
- Location-based services

One way to classify these services depending on the originator of a service session is the ‘Push/Pull' nature. ‘Push' is when the bank sends out information based upon an agreed set of rules, for example your banks sends out an alert when your account balance goes below a threshold level. ‘Pull' is when the customer explicitly requests a service or information from the bank, so a request for your last five transactions statement is a Pull based offering.

The other way to categorize the mobile banking services, gives us two kind of services – Transaction based and Enquiry Based. So a request for your bank statement is an enquiry based service and a request for your fund's transfer to some other account is a transaction-based service. Transaction based services are also differentiated from enquiry based services in the sense that they require additional security across the channel from the mobile phone to the banks data servers.

The other way to categorize the mobile banking services, by the nature of the service, gives us two kind of services – Transaction based and Enquiry Based. So a request for your bank statement is an enquiry based service and a request for your fund's transfer to some other account is a transaction-based service. Transaction based services are also differentiated from enquiry based services in the sense that they require additional security across the channel from the mobile phone to the banks data servers. Based upon the above classifications, we arrive at the following taxonomy of the services listed before.

Table 1.2 : Classification of mobile banking Services

	Push Based	**Pull Based**
Transaction Based		Fund Transfer Bill Payment Other financial services like share trading.
Enquiry Based	Credit/Debit Alerts. Minimum Balance Alerts Bill Payment Alerts	Account Balance Enquiry Account Statement Enquiry. Cheque Status Enquiry. Cheque Book Requests. Recent Transaction History

"The account that travels with the customer". This is needed in today's fast business environment with unending deadlines for fulfillment and loads of appointments to meet and meetings to attend. With mobile banking facilities, one can bank from anywhere, at anytime and in any condition or anyhow. The system is either through SMS or through WAP.

1.10 Technologies Behind Mobile Banking :

Technically speaking most of these services can be deployed using more than one channel. Presently, Mobile Banking is being deployed using mobile applications developed on one of the following four channels.

1. IVR (Interactive Voice Response)
2. SMS (Short Messaging Service)
3. WAP (Wireless Access Protocol)
4. Standalone Mobile Application Clients

IVR – Interactive Voice Response

IVR or Interactive Voice Response service operates through pre-specified numbers that banks advertise to their customers. Customer's make a call at the IVR number and are usually greeted by a stored electronic message followed by a menu of different options. Customers can choose options by pressing the corresponding number in their keypads, and are then read out the corresponding information, mostly using a text to speech program.

Mobile banking based on IVR has some major limitations that they can be used only for Enquiry based services. Also, IVR is more expensive as compared to other channels as it involves making a voice call which is generally more expensive than sending an SMS or making data transfer (as in WAP or Standalone clients).

One way to enable IVR is by deploying a PBX system that can host IVR dial plans. Banks looking to go the low cost way should consider evaluating Asterisk, which is an open source Linux PBX system.

SMS – Short Messaging Service

SMS uses the popular text-messaging standard to enable mobile application based banking. The way this works is that the customer requests for information by sending an SMS containing a service command to a pre-specified number. The bank responds with a reply SMS containing the specific information[14].

For example, customers of the HDFC Bank in India can get their account balance details by sending the keyword ‘HDFCBAL' and receive their balance information again by SMS.

However there have been few instances where even transaction-based services have been made available to customer using SMS. For instance, customers of the Centurian Bank of Punjab can make fund transfer by sending the SMS **‘TRN** (A/c No) (PIN No) (Amount)'. One of the major reasons that transaction based services have not taken of on SMS is because of concerns about security.

The main advantage of deploying mobile applications over SMS is that almost all mobile phones are SMS enabled. An SMS based service is hosted on a SMS gateway that further connects to the Mobile service providers SMS Centre. There are a couple of hosted IP based SMS gateways available in the market and also some open source ones like Kannel.

WAP uses a concept similar to that used in Internet banking. Banks maintain WAP sites which customer's access using a WAP compatible browser on their mobile phones. WAP sites offer the familiar form based interface and can also implement security quite effectively. The banks customers can now have an anytime, anywhere access to a secure reliable service that allows them to access all enquiry and transaction based services and also more complex transaction like trade in securities through their phone [15].

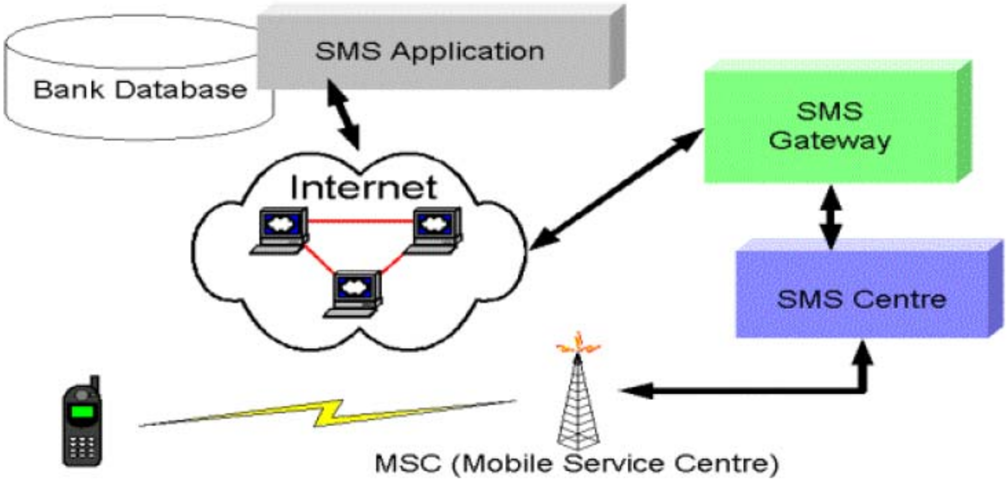


Figure 1.1: SMS Network Architecture

WAP – Wireless Access Protocol

A WAP based service requires hosting a WAP gateway. Mobile Application users access the bank's site through the WAP gateway to carry out transactions, much like internet users access a web portal for accessing the banks services. The following figure demonstrates the framework for enabling mobile applications over WAP. The actually forms that go into a mobile application are stored on a WAP server, and served on demand. The WAP Gateway forms an access point to the internet from the mobile network.

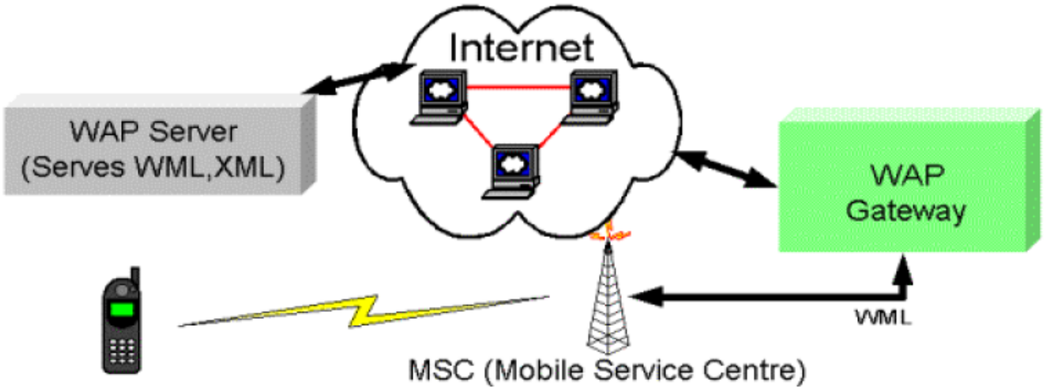


Figure 1.2: WAP Network Architecture for Mobile Applications

Standalone Mobile Application Clients

Standalone mobile applications are the ones that hold out the most promise as they are most suitable to implement complex banking transactions like trading in securities. They can be easily customized according to the user interface complexity supported by the mobile. In addition, mobile applications enable the implementation of a very secure and reliable channel of communication[16].

One requirement of mobile applications clients is that they require to be downloaded on the client device before they can be used, which further requires the mobile device to support one of the many development environments like J2ME or Qualcomm's BREW. J2ME is fast becoming an industry standard to deploy mobile applications and requires the mobile phone to support Java. The major disadvantage of mobile application clients is that the applications needs to be customized to each mobile phone on which it might finally run. J2ME ties together the API for mobile phones which have the similar functionality in what it calls 'profiles'.

Out of J2ME and BREW, J2ME seems to have an edge right now as Nokia has made the development tools open to developers which has further fostered a huge online community focused in developing applications based on J2ME. Nokia has gone an additional mile by providing an open online market place for developers where they can sell their applications to major cellular operators around the world.

Quite a few mobile software product companies have rolled out solutions, which enable J2ME mobile applications based banking. One such product is Wireless Ibanco. The mobile user downloads and installs the wireless I-banco application on their J2ME pone. The J2ME client connects to the wireless I-banco server through the service providers GSM network to enable users to access information about their accounts and perform transactions. One of the other big advantages of using a mobile application client is that it can implement a very secure channel with end-to-end encryption[17].

However countries like India face a serious obstacle in the proliferation of such clients as few users have mobiles, which support J2ME or BREW. However, one of the biggest CDMA players in the Indian telecom industry, Reliance Infocomm has about 7.01 million users all of which have handsets, which support J2ME. Reliance has unveiled one of the most ambitious data services deployment program in the country. On the other hand a country like South Korea with its tech-savvy population has a widespread adoption of the higher-end mobiles, which support application development.

1.11. Mobile Payment Methods

Present mobile payment methods are divided into two classes as “out-of-band” payment method and “in-band” payment method. In the “out-of-band” model, content and operation signals are transmitted in separate channels. This model usually involves a system controlled by a financial institution like bank. In this case, payments involved in the financial transaction are usually macro-payments. Various methods can be deployed to ensure the authentication of payment transaction. In credit card payments, dual slot phone is usually adopted. Other approaches include PIN authentication via a SIM toolkit application and the use of a digital signature based on a public key infrastructure (PKI) mechanism that demand the 2.5G (or higher) technology. Another payment model allows consumers to use SMS text messages to pay for access to digital entertainment and content without being identified. In this application, however, it is the SMS message receiver who is charged, instead of the sender of the SMS message. There are a considerable number of vendors who offer this kind of the reverse-charge/billed SMS service payment models.

In in-band payment method, a single channel is deployed for the transfer of both content and operation signals. A chargeable WAP service over GPRS is of this kind. Two models of this in-bank payment are in use, namely, subscription models and per usage payment models, with the amount of the payment usually being small, that is, micro-payments.

M-payments could be made secure using similar technology to that used in ATM or credit cards, which require a password. Mobile dial-up payments substitute a mobile handset for the merchant's point-of-sale (POS) terminal. The merchant takes the customer's telephone number and telephones a payment request--comprising the telephone number and the amount of the transaction--into the payments platform. When the platform receives confirmation through a call or a Short Message Service (SMS) communication to the customer, the sum is transferred to the merchant's account. To access the server that records and processes transactions, the customer needs no debit or credit card (not always available in emerging markets), only a handset loaded with his or her security-identity-module (SIM) card. The merchant's mobile handset plays the role of POS terminal, but far more cheaply than the real thing.

Mobile scan payments enable customers to pay a merchant directly by scanning their mobile handsets against the merchant's POS reader. The reader uses a radio frequency or Bluetooth (a short-distance, high-frequency radio medium) to communicate with a chip in the handset that authorizes and effects the transaction. If the amount is large, the customer gives a personal identification number (PIN) for authentication. The customer's payments platform will either settle the payment from a "stored-value" account, which the customer can top up by mobile (a prepaid option), or pay on the customer's behalf and send out regular bills (a postpaid option). The transaction time is one or two seconds without PIN authorization and four to seven seconds with it--much faster and more convenient than cash or card transactions.

Remote payments, using a process similar to that for mobile dial-up payments, let the customer pay without being present at the point of sale. A bank would make money from merchants using its mobile-payments system much as it does from "fixed"-payments systems. Telecom companies would gain revenue from the airtime used and from whatever share of the spoils their joint-venture agreement with the partner bank allotted to them. Their core business would also benefit from the indirect value of lower customer churn and cheaper customer acquisition costs.

1.12. Security Issues in Mobile Banking

Mobile personal devices, usually with a built-in display and keyboard, are well-positioned to provide a technical solution for reducing fraud and allowing the fair allocation of responsibility for damages from fraud. Some amount of security is already part of the authentication mechanism of existing mobile phones as a way to prevent call theft. Moreover, it is relatively easy and inexpensive for device manufacturers to incorporate additional mechanisms to ensure secure transaction authorization. These mechanisms help prevent most fraud and allocate responsibility fairly for any remaining fraud. For users, their value far outweighs their relatively modest cost [18].

Secure transactions using mobile phones consist of four independent processes :

1. Identification process : The device identifies the user through physical possession (as with regular mobile phones), passwords, or biometrics (such as voice recognition);
2. Authentication process : The mobile banking service provider authenticates the transaction request from the device via either subscriber identification (as with existing phones) or cryptographic mechanisms such as digital signatures or secure protocols, like the Wireless Transport Layer Security Specification;
3. Secure performance : The financial transaction is performed by the mobile banking service provider, possibly with the help of the merchant and/or other transaction provider(s) for bill payments and may involve secure payment protocols (such as Internet Keyed Payments/Secure Electronic Transactions, or iKP/SET)[19].
4. Confirmation : A confirmation of the completed transaction is delivered to the user.

Mobile phone devices should incorporate mechanisms to securely authenticate transaction requests that can be used by multiple transactions and scenarios. To allocate responsibility, transaction requests should be digitally signed by the device using a private key (not known to the providers) kept in the device. The user does not have to obtain a public-key certificate from a trusted certificate authority; it suffices that the agreement between the user and the provider states the public key and the algorithm. To reduce hardware costs, designers may prefer public-key signature algorithms (such as the Digital Signature Algorithm, or DSA (Digital Signature Standard, 1994 [20]), so most of the computations are done offline, and online signing is efficient.

The device displays the transaction details to the user and asks his or her consent for each transaction request. The device should ensure the user is aware of the entire request, possibly by limiting the request format. For example, payment transactions may display the amount and other transaction details related to that particular financial service.

The security of this design depends on the secure operation of the mobile personal device, including its user identification. Some current mobile devices, including phones, use only simple, preprogrammed processors, and therefore can be trusted to operate securely. However, some devices support downloaded, general-purpose applications and like computers, may be vulnerable, as with viruses.

Secure transaction authorization may, therefore, involve a secure coprocessor, used only to authorize transactions and possibly to view confidential data. There should be visible indication when the display and keyboard are controlled by the secure co-processor, allowing the user to securely identify (such as by password) and authorize transactions. The co-processor is invoked by the main processor to authorize transactions, providing the raw request in shared memory. If authorized, the co-processor returns the signed transaction request in the shared memory.

The simplest secure transaction architecture involves only the user, the device, and a single transactions provider (such as a bank, brokerage, or insurance company). The user identifies to the mobile device, possibly through secure identification mechanisms (such as a PIN, voice identification, or fingerprint); the device then authorizes a transaction to the provider (such as money transfers and investments). Authorization is preferably through some secure public-key signature process, allowing precise allocation of responsibility for fraud (disputed transactions). However, less secure forms of authorization (such as relying on subscriber identification and/or encrypted passwords) may suffice for some applications, as in e-banking and mobile commerce solutions.

More complex payment transactions such as mobile purchasing typically involve at least one additional party, the merchant. In the simplest case, the merchant receives payment from external payment/transaction provider (such as a bank or credit card company); the mobile transaction provider authorizes the transaction.

Wireless communication capability supports mobility for end users in mobile banking systems. Wireless LAN and WAN are major components used to provide radio communication channels so that mobile service is possible. In the WLAN category, the Wi-Fi standard with 11 Mbps throughput dominates the current market. It is expected that standards with much higher transmission speeds, such as IEEE 802.11a and 802.11g, will replace Wi-Fi in the near future. Cellular networking technologies are advancing at a tremendous pace and each represents a solution for a certain phase, such as 1G, 2G, and 3G, in a particular geographical area, such as the United States, Europe, or Japan.

Compared to WLANs, cellular systems can provide longer transmission distances and greater radio coverage, but suffer from the drawback of much lower bandwidth (less than 1 Mbps). In the latest trend for cellular systems, 3G standards supporting wireless multimedia and high-bandwidth services are beginning to be deployed. WCDMA and CDMA2000 are likely to dominate the market in the future.

1.12.1 Frauds in Present Technology Environment

With banks deciding on setting up networks and computerize the whole banking process, to offer their services on multiple channels, they now face risks both from inside and outside. This section describes the kind of frauds that can happen in this environment.

Some more avenues for frauds in this emerging banking scenario :

- **Mail Spoofing** – E-Mail Forgery: sending wrong information to bank customers as if its from authentic bank sources
- **Web Spoofing** – Web Site Forgery: Diverting the customers of a bank to an exactly duplicated forged web site and impersonating those customers on real bank site
- **Attacking the User Computer**: To take control of that machine
- **Attacking a Bank's Server**: To take control of that machine
- **Media Tapping** – recording the whole transactions of a bank, or customer etc and replaying the same for their advantage
- **Denying Service**: Though the server is available, making it not able to render service, by poisoning the Network Infrastructure.

Prevention

A close observation reveals that all frauds happen due to impersonation, sniffing information on its travel and hacking into the computer. The impersonation can be for an individual, a web site, a computer, a router etc. The frauds due to impersonation, sniffing can be minimized by adopting PKI – Public Key Infrastructure. Frauds due to hacking and not able to deploy PKI, etc. can be minimized by firewalls, IDS – Intrusion Detection System.

1.12.2 Device related issues and Security risks in SMS banking :

User and device authentication

The SMS Mobile Banking application is bound to each deployment of SMS Enterprise server application in turn making it bound to the bank's server [21]. Whenever an SMS Mobile Banking application is issued to the user, the bank's public key is embedded inside the application. This application is set up in a closed user group setting to accept signature messages only from the bank's server. On installation on the mobile handset of the authorized user, the application would generate a key pair comprising a public key and private key automatically. These keys would be bound to the mobile number of the device and the user defined password (known only to the user). The user would send the device public key using the application interface through an encrypted SMS to the bank's central key repository. To add another layer of security the keys are stored on the bank's server in encrypted form.

Password Security on the device

Wireless banking increases the potential for unauthorized use due to the limited availability of authentication controls on wireless devices and higher likelihood that the device may be lost or stolen. Authentication solutions for wireless devices are currently limited to username and password combinations that may be entered and stored in clear text view (i.e., not viewed as asterisks "****"). This creates the risk that authentication credentials can be easily observed or recalled from a device's stored memory for unauthorized use. In SMS Mobile Security application on the handset/PDA, every time the user needs to use the application or any of its features he/ she has to enter the unique password (known only to him / her – not even the bank). There is no specific requirement for a password / PIN that the user gets from the bank.

Authenticating initial users and existing customers

Digital Signing and verification

Verifying a customer’s identity, especially that of a new customer, is an integral part of all financial services[22]. In addition to the initial verification of customer identities, the financial institution must also authenticate its customers’ identities each time they attempt to access their confidential information. Financial institutions need to weigh the cost of the authentication method, including technology and procedures, against the level of protection it affords and the value or sensitivity of the transaction or data to both the institution and the customer.

Authentication methods that depend on more than one factor are typically more difficult to compromise than single-factor systems therefore suggesting a higher reliability of authentication. SMS Mobile Solution involves the following authentication and verification mechanisms (factors):

- Something the user possesses – The mobile device with the bank’s application bound to the user’s device.
- Something only the user knows - A user defined password.
- Something that binds each message to the user – The SMS message which contains the user’s transaction information is bound to the user through user’s digital signature (user’s private key is used for signing the SMS message).

Secure Inter bank settlement

Once the user’s inputs are received securely at the bank’s server through SMS Mobile Banking Solutions, the bank’s server would interface with its core banking infrastructure as well as other participating banks for the background settlement. It is assumed that appropriate security controls existing within the banks infrastructure would provide for intra as well as inter bank transfer and settlements / information notifications.

1.13 Cost Versus Security

Security measures are needed to prevent certain risks and associated costs to occur. The security measures, however, also impose a certain cost by themselves. A proper balance should therefore be made between the investments in security measures and the potential costs that a bank might have to cope with due to remaining risks without these measures. Particularly in electronic banking systems, the extra cost at the client side is reduced as much as possible. Users should be able to perform electronic banking with the standard infrastructure and software that is already available. This makes the electronic banking service more attractive, but might unfortunately have an impact on the security level this service can offer. In practice, banks try to have a minimal level of security alleviating most of the risks, with maximum level of convenience.

Let us consider a fictitious electronic banking system. Four major functionalities are present in our fictitious bank. As separation of concerns increases the modularity, maintainability, etc., and as such security, these functionalities are implemented as four distinct services:

(1) To interact with clients, the bank requires an Interface Server. An interface is needed for all different environments: ATM, WWW, and WAP.

(2) The bank should verify the authenticity of client requests and should authenticate its responses. This is done by the Authentication Server.

(3) Financial transactions are validated by the Transaction Server. This server also provides an easy interface towards the mainframe.

(4) Finally, the Mainframe executes the transactions and keeps the financial records.

This structure reflects the different services that are present in any electronic banking system worldwide. The security of the communication between the client and the bank is handled in the Interface Server part. The authentication of the user is handled by the mobile device & Authentication Server.

Note that it would be possible to rely on a third party to provide for example the authentication service. Microsoft's Passport [23] is such a service that is intended to provide a single identity with which a user could perform all its online activities. Although this might work for some e-commerce merchants, authentication in an electronic banking application is far too critical to entrust it to another party.

1. 14 Communications Security

The standard solutions that are used within almost all electronic banking systems, namely SSL/TLS and WTLS, for Internet and WAP banking respectively are discussed below.

1.14.1 SSL/TLS/WTLS in general

Secure Sockets Layer (SSL) was originally an initiative of Netscape. The IETF adopted SSL for its Transport Layer Security (TLS) protocol [24]. The WAP Forum adapted TLS to create a wireless equivalent, Wireless Transport Layer Security (WTLS) [25]. Detailed background information on SSL/TLS can be found in Rescorla [26]. Although there are differences between (several versions of) these protocols, conceptually they provide the same security service: a secure channel between client and bank.

1.14.2 Secure Channel

SSL/TLS/WTLS provides a secure communication channel between the client and the bank. This means that the data that is transmitted between both ends is kept secret (confidentiality) and that tampering will be detected (data integrity); the bank is always authenticated; the client can be required to authenticate too. Note that many electronic banking systems do not rely on the client authentication feature of the secure channel, but rather implement a client authentication mechanism on top of this channel.

An advantage of SSL/TLS/WTLS is that it can easily be used underneath various communication protocols, including but not restricted to HTTP. As SSL/TLS/WTLS only provides a secure channel, it does not provide non-repudiation: at the receiving side, the transmitted data leaves the secure channel, and the cryptographic protection is removed; there is no digital signature on client data. Electronic banking systems should therefore implement a non repudiation mechanism on top of the secure channel. However, note that this is rarely done in practice.

1.14.3 Handshake and Data Transfer

A connection between the client and the bank is divided into two phases, the handshake and the data transfer. The purpose of the handshake is three-fold [27]: client and bank need to agree on a set of cryptographic algorithms that will be used to protect the data, to authenticate each other, and to agree on cryptographic keys; secondly, they need to establish a set of cryptographic keys with which data will be protected; lastly, the bank authenticates to the client and, optionally, the client authenticates to the bank.

Once the handshake has been completed, data transfer can take place. Data is broken up in fragments, and transmitted as a series of protected records. To provide data integrity, a Message Authentication Code (MAC) is computed over a data fragment; fragment and MAC are then encrypted.

1.14.4 SSLv2/SSLv3/TLS

The first public version of SSL, version 2, suffered from a number of security flaws, which have been fixed in SSLv3. As browsers nowadays still support SSLv2, and as it is still in use in some systems [26]. The same cryptographic keys are used for message authentication and for encryption; this means that in export mode the security of the MACs is unnecessarily weakened. SSLv2 has a weak MAC construction and relies solely on the MD5 hash function; Dobbertin has demonstrated the vulnerabilities of MD5 in [28]. SSLv2 does not have any protection for the handshake; hence a person-in-the-middle attack cannot be detected. Finally, a truncation attack is possible, as SSLv2 simply uses the TCP connection close to indicate the end of data, so that the attacker can simply forge the TCP FINs and the recipient cannot tell that it is not a legitimate end of data [27].

1.14.5 WTLS

The WAP Forum has adapted TLS to make it suitable for a wireless environment with small devices, which have limitations on bandwidth, memory and processing [27]. WTLS therefore includes the usage of elliptic curve cryptography (limited memory and processing) by default; WTLS does also work on top of a datagram instead of a connection based communication layer (compare to UDP vs. TCP on the Internet); finally, WTLS defines its own certificate format optimized for size (limited bandwidth), but supports the ordinary X.509 certificate too.

1.15 Client Authentication

Providing a secure communications channel from a client to an authenticated bank is only part of a secure electronic banking system. Authenticating the client & his mobile device is the other crucial part.

1.15. 1 Entity vs. Transaction Authentication

An important distinction should be made between entity and transaction authentication. Entity authentication means that the client authenticates when initiating a session with the bank. Transaction authentication means that individual transactions within this session are authenticated by the client. Depending on the authentication mechanism, transaction authentication can provide non-repudiation of single transactions, while entity authentication does not provide non repudiation of transactions. This distinction is clearly made in today’s electronic banking systems worldwide. In some systems only entity authentication is present, while other systems incorporate transaction authentication too. Both entity and transaction authentication can be provided in various ways.

1.15. 2 Authentication Mechanisms

1. Fixed Passwords

Many electronic banking systems all over the world still rely on a fixed password to authenticate the client. This password can be a PIN number or a character-based password, and is often combined with a service account number that is not easy to guess (i.e., unrelated to the user’s name or bank account). In many cases only a subset of the digits has to be provided by the user, which provides some security against an attacker who is looking over the shoulder or is sniffing the keyboard (the bank asks for a different subset each time).

Fixed passwords are very often used for entity authentication. In rare cases they are also used for transaction authentication, although this is rather entity authentication for a single-transaction session. In many systems fixed passwords are used for entity authentication. Moreover, a password is almost always required to bootstrap the system the first time the user starts using it. This is typically different from the password(s) used in the normal sessions. Passwords should never be sent in clear over the network. They are, however, also vulnerable to dictionary attacks, password guessing, and social engineering. Although these risks have been known for a long time [29], fixed passwords are still widely used, for they are very easy to implement and use.

2. Dynamic Passwords

Banks sometimes issue a list of one-time passwords to their users. These can only be used once, and should therefore offer more security. However, it is very difficult to learn these by heart, and so the users will be forced to keep a list somewhere either on paper, or worse, on a file on their PC. Terminology banks use includes ‘scratch list number’, mostly used for entity authentication, and ‘transaction number’, used to authenticate individual transactions. Some systems use a combination of fixed and dynamic passwords: fixed for entity authentication and dynamic for transaction authentication. Instead of issuing a list of independent passwords, it is possible to generate a chain of dependent one-time passwords; see for example the system described by Haller et al. in [30] which is based on an idea described by Leslie Lamport in [31]. This usually requires extra software at the client side.

3. Challenge/Response

The idea of a challenge/response scheme is that the client proves his identity to the bank (i.e., entity authentication) by demonstrating knowledge of a secret, not by just sending this secret to the bank, but by producing the proper response to a random challenge using this secret. There are symmetric and asymmetric challenge/response schemes. In a symmetric scheme for example, the response consists of a MAC on the time or on a random challenge of the bank. A digital signature on a random challenge message is an example of an asymmetric scheme. These challenge/response schemes are often implemented with hardware tokens.

4. SSL/TLS/WTLS

Using a digital signature for a challenge/response scheme is actually an option in the SSL/TLS/WTLS protocols. When setting up a secure channel between the client and the bank, the client can also be authenticated explicitly using a digital signature: during the handshake, the client signs a hash of all the previously exchanged handshake messages. Usually, the private signing key is stored on the user’s mobile device and is only protected with a password. Note that due to constraints in current WAP phones, this is not yet practically used in WAP banking systems.

5. Digital Signature

Besides entity authentication, digital signatures can also be used for transaction authentication. This is the most secure alternative. However, of today’s browsers, only Netscape includes a JavaScript mechanism to digitally sign, for example, the contents of a form. So, electronic banking systems normally use their own implementation, a standalone application or an applet, for digital signatures.

As indicated before, the private signing key is usually stored on the user’s mobile device and is only protected with a password. Moreover, Shamir and van Someren [32] have shown that cryptographic keys are very vulnerable in software. This has been successfully verified by

Janssens et al. in [33]. Still, the level of security is substantially higher than when using fixed passwords.

6. Hardware Tokens

Several of the previously discussed mechanisms can be (more securely) implemented using hardware tokens.

Private digital signature keys for transaction authentication can be kept on smart cards. Due to the cost of issuing extra smart cards to users, this highly secure solution is not frequently deployed in Iran. However, existing smart card applications can be and are used as a means for entity authentication, e.g., electronic purses, or an electronic identity card.

Hardware tokens which display a response to the current time interval (e.g., SecurID [34]) or to an unpredictable challenge given by the bank via the computer screen and typed in by the user on the token (e.g., Digipass [35]), are used for entity authentication. These hardware tokens can sometimes also calculate MACs for the purpose of transaction authentication.

Mobile devices such as PDAs or special-purpose wireless wallets can enhance an Internet or WAP banking system's security. These devices are considered personal, and can perform cryptographic protocols, to provide both entity and transaction authentication. The communication between the device and the PC or WAP phone is realized manually, with Bluetooth [36] or with an infrared interface.

The compromise of one token could lead to the disastrous scenario in which the bank should issue a new token to all users. To prevent this, all tokens should contain a different cryptographic key. When using asymmetric keys this is not a problem. However, in the case of symmetric keys, it requires the maintenance of a secure database containing all the secret keys the bank shares with its users. Symmetric keys are therefore often cryptographically derived from a unique serial number of the token and a master key that is the same for all (or a subset of all) the tokens. In this way, each user shares a different key with the bank, without the problem of the secure database.

1.16 Additional Security Issues

Communications security, i.e., a secure channel between a client and an authenticated bank, and client authentication, i.e., entity and transaction authentication, are the two main security issues present in an electronic banking system [37]. There are, however, some additional security issues, which unfortunately in practice are sometimes the most critical ones.

1. Registration

Before a user can actually use a secure mobile banking system, a registration procedure is performed. During this registration procedure, the security of the system is bootstrapped: the user has to obtain an initial means for entity authentication, with which a first secure session can be established with the bank; thereafter, the regular security authenticators are enabled. Usually an initial password is used which the user obtained via paper mail, and/or after having physically authenticated in one of the bank’s offices. Sometimes, user authentication via the phone is required at the first login at the bank’s system; the user then for example has to give the operator a challenge displayed on screen, and/or answer some questions. It is clear that if something goes wrong during this stage, the security of the rest of the electronic banking system is undermined.

2. Delegation

In some situations, the ability of delegation within an electronic banking system is desired. For example, the manager of a department would like to be able to delegate (restricted) rights to one or more employees who need to have access to the banks banking transactions, or possibly parents would like to delegate certain rights to their children.

If the authentication of the client is only based on a fixed password, delegation can unfortunately be performed by just sharing the password. However, this is not delegation but rather impersonation. If client authentication is more secure, it is more difficult to give away the necessary secret information, or at least, it is difficult to duplicate it, for example in the case of smart cards.

A small number of existing electronic banking systems in worldwide implement some kind of real delegation mechanism. For example, the owner of a bank account can create additional password-protected accounts with limited rights.

3. Secure Platforms

When discussing the establishment of a secure communications channel between a client and the authenticated bank, and the authentication of the client, the assumption has to be made that the user’s mobile device, operating system, and software form a secure end-point in this process. Critical trusted anchors are not always present. Typical client platforms have shown to be very vulnerable, as described by Loscocco et al. [38]. Viruses, Trojan horses, worms, and other malicious programs can tamper with the installed root certificates, they can steal a user’s private keys, they can spoof the user interface or mislead users in another way, they can intercept communication before it is securely sent to the bank, etc.

Even smart cards may not protect against this problem. If the card is unlocked by typing a PIN code via the ordinary keyboard, the PIN code could be captured or the user could be requested for the PIN code through a fake interface. Ideally, a smart card reader should therefore have its own pinpad and a small display. Users do not have to enter PIN codes via their mobile device then. Users are then also able to verify crucial information on a trusted display. Common specifications for such secure readers are being developed [39]. However, it still constitutes an expensive solution. Most current smart card readers therefore only consist of a slot in which the card can be inserted. This still protects the card’s private key itself, but does in theory not prevent access to the card’s signing function.

An industry alliance has been working on mechanisms that provide more trust and enable security on an end-user’s computing platform [40]. This effort in particular enables a more secure creation of digital signatures on an end-user’s computing platform [41].

Also the bank’s server should form a secure end-point in the electronic banking system. The appropriate measures should be taken to prevent hackers from breaking into the site. A detailed information can be found in Garfinkel and Spafford [42].

4. The Human Factor

The fact that a client platform is not secure is often just due to the lack of security knowledge of the end-user. Although the typical client platform is inherently insecure, most problems could be prevented by an educated, careful, and security-conscious user. Mobile banking users should keep their security authenticators, whether these are just passwords, a list of one-time passwords, hardware tokens, or the PINs to unlock these tokens, private, and protect them from potential abuse. Users should install virus scanners, and keep them and their system up-to-date. Users should avoid practices that easily lead to security hazards; in particular they should not start up arbitrary executable attachments received via electronic email. Users should check fingerprints of certificates against the fingerprints that are (should be) given by the bank on official paper documents. Online Banks should provide information to their users about these matters. In fact, they mostly do this to be able to decline responsibility in case something goes wrong and it turns out it is due to the user. The bank’s system administrators should be properly trained in computer security. They should for example regularly monitor security advisories and apply software patches when required.

5. Logging and Monitoring

The previous sections made clear that there is no such thing as perfect security. No matter the amount and strength of security measures in place, there will always be remaining potential security weaknesses. As some security breaches cannot be completely prevented (e.g., obtaining and misusing a user’s credentials), logging and monitoring will allow the online bank to at least detect security hazards, or find out later what exactly happened. These detection mechanisms can go from just passive logging to active monitoring, e.g., sending an alert to the bank if certain transactions do not match a user’s regular profile[43].

1.17. Research Issues in this Study

The growth of mobile phone subscriber base is increasing in an exponential manner. It is predicted that all inhabited areas (and hence the entire population) of India would be covered by mobile networks by the end of 2012, despite only 65-70 per cent coverage today. The number of total mobile subscribers is expected to increase to over 600 million by year-end of 2012. This will support the usage of mobile devices for various kinds of online business and also financial transactions. In this scenario, the Indian banks have to be equipped to start online banking channel as new distribution channel. But, presently, the acceptance of mobile banking services by the customers is not encouraging. It is necessary to find the reason for slow penetration of this value added service in the country. Hence it is planned to study the technological aspects, business model, various security issues and possibility of improvement in providing security and authenticity for online financial transactions.

The motivation behind this study are to analyze the significance of usage of mobile device for online financial transaction and to identify the gap between mobile communication technology innovations, their penetration in banking industry as a new distribution channel and the customer acceptance. This also include to suggest a suitable model for secured financial transaction for ubiquitous banking.

Following research issues are discussed and analyzed :

☛ Opportunities and challenges for mobile business.

☛ Significance of mobile business activity in financial sector with special emphasis in banking sector.

☛ To study and analyze the mobile banking technology models like SMS banking and WAP banking.

☛ To study the requirement for next generation payment system.

☛ To study the security architecture of GSM and GPRS.

☛ To provide enhanced security through biometric authentication.

☛ Customer’s perspective on mobile banking adoption and its effect on intention and behavior of usage of mobile banking services.

☛ To propose a suitable business model for mobile business through mobile payment to take care of security and authentication problems.

Chapter II

Review of Literature on Mobile Business Technology, Mobile Banking Services, & Security

2.1. Introduction

Current wireless devices include phones, hand-held or palm-sized computers, laptops, and vehicle-mounted interfaces. In order to be easily carried, these mobile devices must be physically light and small. In addition, a mobile device should be a multiple-purpose device so that a user does not have to carry other appliances. While achieving mobility, mobile devices suffer from some drawbacks compared to personal computers. They have (1) small screens and small multifunction key pads; (2) less computational power, limited memory and disk capacity; (3) shorter battery life; (4) complicated text input mechanisms; (5) higher risk of data storage and transaction errors; (6) lower display resolution; (7) less surfability; (8) unfriendly user-interfaces; and (9) graphical limitations. In addition to these device limitations, there are technical restrictions related to the wireless network. As compared to wired networks, wireless communications add new challenges: (1) less bandwidth, (2) less connection stability, (3) less predictability, (4) lack of standardized protocol, and (5) higher cost.

Mobile business is enabled by a combination of technologies such as networking, embedded systems, databases, and security. Mobile hardware, software, and wireless networks enable mobile business systems to transmit data more quickly, locate users' positions more accurately, and conduct business with better security and reliability. In this chapter, the key technologies that make mobile business a reality and that will improve its performance and functionality in the near future are discussed. This includes review on mobile communication technology, information exchange technology, location identification technology, and security considerations. The chapter also contains an overview mobile communication devices. Technological aspects of various mobile payment technologies are also discussed with their advantages and limitations. Literature review on the various research issues like Online banking, Significance of mobile business activity in financial sector with special emphasis in banking sector, and Security issues on mobile banking transactions are included. Finally a review on mobile payment including various threats and vulnerabilities are presented.

2. 2. Mobile Communication Technology

Though Internet access is available in most major cities and many rural areas, the Internet connections for many businesses, homes, and schools use relatively slow modem connections through Internet Service Providers (ISPs). Making high-speed (broadband) connections directly available to all locations is the key to realize the true benefits of mobile business applications. A number of existing or future technologies that enable connections between mobile devices and other information appliances, and between mobile devices and the Internet, are discussed below:

2.2.1. First-generation (1G) networks : Less often used than the following terms, 1G denotes the very first generation of common mobile communication networks connectable to the Public Switched Telephone Network (PSTN). These were analog cellular systems such as Advanced Mobile Phone System (AMPS) in the USA, Nordisk Mobiltelefon (NMT) in Scandinavia, or C-Netz in Germany. 1G technologies embodied the first realization of cellular concepts, including frequency reuse and handoffs.

2.2.2. Second-generation (2G) network : GSM (Global System for Mobile Communication) is considered the second-generation (2G) digital network. It is a circuit-switched service, where users must dial-in to maintain a connection when data communications are desired. It operates in the 900 MHz and 1,800 MHz frequency bands, and is widely used in Europe and Asia. Other 2G networks are Digital AMPS (D-AMPS) in the USA, Code Division Multiple Access (CDMA) in USA and Japan, and Personal Digital Cellular (PDC) in Japan. Major functional enhancements of 2G technologies are voice coding, digital modulation, and forward error correction. Additional services like fax, data, messaging, and roaming between networks were provided. Especially in the GSM case, the successful Short-Message Systems (SMS) service has shown that voice traffic is not the only service users want. The standardization of the Wireless Application Protocol (WAP) brings the first phones with an integrated browser onto the market. These 2nd generation systems had such a wide impact due to the rapid reduction in costs and the perceived quality.

2.2.3. 2.5G network : GPRS (General Packet Radio Service) are so-called 2.5G technologies. GPRS, based on GSM, is a continuous packet data service. It uses the existing network infrastructure but is being marketed as delivering ISDN-type speeds. Rather than sending a continuous stream of data over a permanent connection, GPRS's packet switching system only uses the network when there is data to be sent. Users can send and receive data at speeds of up to 115 kbits / second with GPRS. From the revolution intensity point of view, there are many industry opinions expecting 2.5G networks to represent the most remarkable change [44] (The Boston Consulting Group, 2000).

2.2.4. 2.75G network : Whereas 2.5G technologies introduce a set of packet-switched functionalities and minor changes of transmission speed only, 2.75G denotes 2.5G technologies with major improvements in transmission speed. EDGE (Enhanced Data GSM Environment), a faster version of GSM, is designed to enable the delivery to multimedia and other broadband applications. It will use new modulation techniques to enable data rates of up to 384 kbits/second over the existing GSM infrastructure. CDMA networks are upgraded to the first versions of cdma2000 [45](Autio et al., 2001).

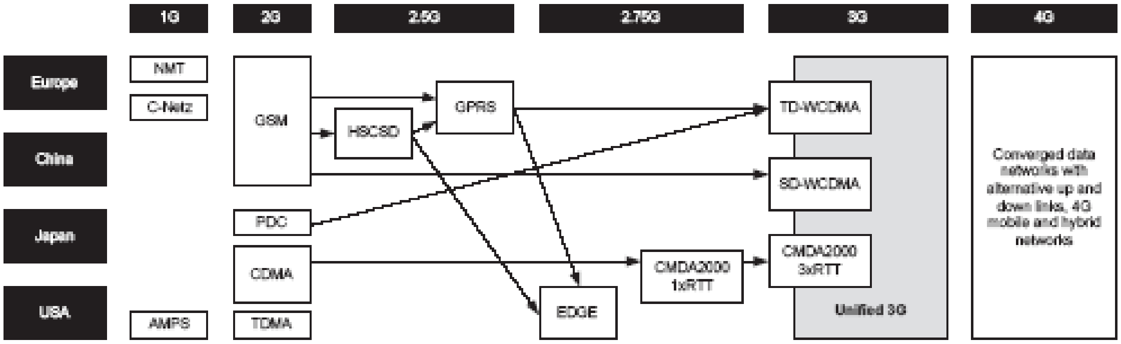


Figure 2.1: Wireless network technology evolution [45](Autio et al., 2001)

2.2.5. Third-generation (3G) network : UMTS (Universal Mobile Telecommunications System) is the so-called "third-generation (3G)" technology. It aims to offer higher-bandwidth, packet-based transmission of text, voice, video, and multimedia needed to support data-intensive applications. Once UMTS is fully implemented, computer and phone users can be constantly connected to the Internet and have access to a consistent set of services worldwide. Integrating the functions of a whole range of different equipment, the new 3G mobile phone can be used as a phone, a computer, a television, a paper, a video conferencing center, a newspaper, a diary, and even a credit card. There are two major competing schemes for UMTS. Wide band-CDMA (W-CDMA), which is supported by Nokia and Ericsson among others, and time division-code division multiple access (TD-CDMA). W-CDMA is similar to standard CDMA except that it uses higher bandwidth on the transmission channel. TD-CDMA is a scheme that makes use of both TDMA and CDMA techniques. 3G technologies can support data rates from 384 kbps up to 2 Mbps. Auctions for 3G spectrum licenses occurred in a number of countries in 2000 and the first commercial offerings of 3G services began in Japan in October 2001. More recently, Verizon Wireless has started offering ‘‘3G’’ service in portions of its serving territory (although this is not true-3G service). Fundamental changes are required on the terminal side, as the terminal is drifting away from the classic telephone, and going towards smartphones, Personal Digital Assistants (PDA), and Pocket Computers. An obvious need for software platforms rises, and several Wireless Operating System (Wireless OS) approaches already exist.

2.2.6. Fourth Generation (4G) Technology : Mobile services, applications, and even core network are evolving at high speeds, and distinguishing different generations is not really possible anymore. The evolution and sometime revolution, is a very significant trend and 4G is such a revolution of air interface rather than new phase of evolution. The Japan's leading mobile phone company NTT, DoCoMo's next target is to achieve a speed of 100 million bits per second for 4G by 2010. 4G technology is characterized by advanced personalization, Industry specific e-process models, Optimized CRM, and Niche customization. E-marketplace is an evolving example of a parallel to a true 4G enterprise business environment. 4G technology provides Web transformation through external automation. The various external automation technology may involve High optimization, Niche customization, Transparent processes, Self-service, Any –to-any multi-channel integration, Advanced personalization, Voice customer service, E-process driven technology, and Architectural interoperability. The various 4G initiatives are very recent. Most of these set out to achieve the performance that 3G initially intended to provide, but the focus remains on the convergence between existing networks. The use of the 4G term remains questionable and open for discussion, since no real revolution in convergence between telecommunication and data communication is expected after the third generation. On the other hand, deployments of all-IP based wireless networks might originate from operator independent developments. Simply increasing performance, speed, quality, etc.—as long as it can be described within the 3G service space dimensions, could still be regarded as development of 3G technologies.

2.2.7. The 3G Service Space

The next generation of wireless and mobile technologies is the third generation (3G). There is a large diversity of parallel development trends in related technologies, and one might argue that there is no common way to summarize these trends. However, the 3G technology trends can be described by three fundamental dimensions, which together form the 3G technology space or the 3G service space [46](Rasanen, 2001) :

The 3G service space can be identified by the space as spanned by the following set of abstract dimensions:

- Terminal capabilities,

- Bandwidth,
- Packet data service.

The parallel, mostly independent development of wireless terminal capabilities, wireless transmission bandwidth technologies, and wireless packet data functionality enable 3G solutions, services, and applications. Although there might be some 3G technologies which only benefit from one of the three dimensions, most technologies are dependent on at least two of the three dimensions. The real 3G value results from an environment with increased terminal capabilities, increased packet data support, and increased bandwidth. For avoiding misleading use of the 3G terminology, we define it such that if a solution cannot be explained by and located in the 3G service space, it should not be considered as related to 3G (figure 2.2) [47](Lin et al., 2001).

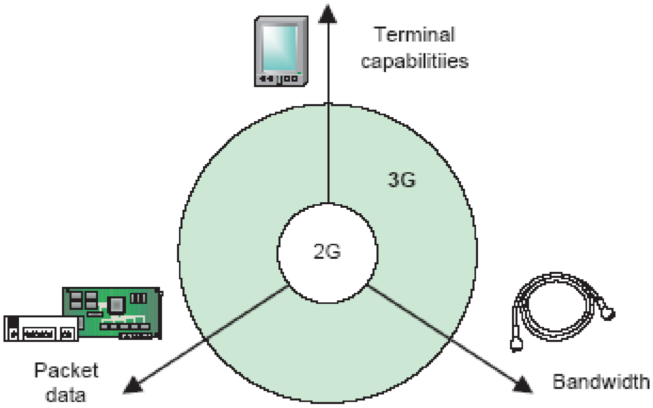


Figure 2.2: From 2G to 3G in three dimensions: the 3G service space

2.2.8. Universal Mobile Telecommunications System :

With remarkably higher transmission rates, the Universal Mobile Telecommunications System (UMTS) delivers true universal multimedia coverage and nationwide roaming. More than that, UMTS offers greater spectrum efficiency and capacity compared to the current 2G and 2.5G networks. UMTS is intended to be a solution for managing increasing and converging demands for mobility, data, and multimedia. Due to the absence of global standardization in the early ages of wireless communication, there are today two major regional telecommunication standards dominating the global market, TDMA/CDMA developed by TIA in the USA and GSM developed by ETSI in Europe. Moving toward 3G wireless, there has been a rising need to develop more global and collaborative standards [48](Patel and Dennett, 2000).

2.2.9. Information Exchange Technology

Information is at the heart of any system that makes use of mobile devices and telecommunication technology. The current methods for information exchange in mobile application rely on standards supported by the wireless infrastructure.

1. HTML-based Information Exchange Standards : HTML (Hyper-Text Markup Language) is widely adopted by the Internet community as the document format for browsing. The availability of authoring tools and browsers makes it easy for users to create HTML documents incorporating multimedia objects. Although HTML is not a suitable format for information exchange in the wireless domain, a compact version of HTML, known as cHTML, has been used in the NTT DoCoMo's iMode services.

2. XML-based Information Exchange Standards : eXtensible Markup Language (XML) tags data and puts content into context, and thus enables content providers to encode semantics into their documents, eXtensible Stylesheet Language (XSL) works to transform XML data into structured documents such as HTML. XML and XSL work together to allow the complete separation of content from layout information. However, XML and XSL alone are not enough to provide the compact information exchange required by mobile business applications. To address this shortcoming, Wireless Markup Language (WML) has been derived from XML. WML allows information to be represented as cards suitable for display on mobile devices. WML has also been adopted by WAP as the format for information exchange.

2.2.10. Location Identification Technology

In mobile communication, knowledge of the physical location of a user at any particular moment is central to offering relevant service. Location identification technologies are important to certain types of mobile business application, particularly those whose content is varied depending on location. Global Positioning System (GPS), a useful location technology, is a system of satellite stations used to calculate geographic location with great accuracy. It is widely used and will also play an important role in wireless communication.

2.2.11. Network Problems

1. Network incompatibility : Multiple, complex and competing protocols exist in today's cellular network standards. TDMA (time-division multiple access) was chosen by many cellular networks equipment suppliers and network operators in the early 1980s when cellular networks were first introduced in the U.S. CDMA (code division multiple access) was adopted later by other operators for its greater capacity. GSM is used as a single technical standard for the network operators in Europe, and it has become the standard used by most of the world's cellular subscribers. These different standards have resulted in a global incompatibility of cellular handsets.

2. Bandwidth access : The Federal Communications Commission (FCC) has established several frequency bands for use by cellular network operators across the country. In order to encourage competition, the FCC prohibits cellular operators from owning more than 45 MHz of radio spectrum in a given geographic region. Known as the "spectrum cap", this regulation imposes barrier for U.S. cellular network operators who are attempting to implement the new high-bandwidth, next-generation networks.

3. Responsibility and control : The mobility enjoyed by m-business also raises very important responsibility and control issues. While the technology ensures transmission security between the phone and the base station, it does not cover the rest of the network infrastructure. Though most wireless data networks today provide reasonable levels of encryption and security, serious consideration must be given to the issue of security as we move towards a mass-market adoption of mobile business applications.

2.2.12. Infrastructure Tasks

1. Lack of a standardized Web language : Today's mobile devices utilize a broad range of often incompatible standards, making the process of creating a successful m-business application even more difficult. While newer mobile phones will incorporate WAP and its Wireless Markup Language (WML), NTT DoCoMo's iMode uses condensed HTML. Since numerous standards exist, the standardization issue is a complex one to manage, and may affect mobile business adoption.

2. Seamless integration : The integration between network operators and businesses is another key issue for mobile business. While location-based services will make it possible for a carrier to know where you are, the problem of privacy has simultaneously emerged. At the same time, the carriers, who will likely be asked to provide the same level of quality service for their wireless networks as for their wired data service, will be faced with legal concerns.

3. Support services : To conduct business via mobile devices, a company must be capable of managing and supporting a large base of mobile customers or employees. This poses a challenge to the traditional helpdesk and customer care function. On one hand, the company must deal with the logistics, procurement, and asset management issues surrounding large numbers of devices and software. On the other hand, the broad range of mobile devices makes customer care far more complex and harder to manage.

2.2.13. Security Considerations

As a new way of conducting business, mobile business must tackle security issues in its implementation. Mobile business has to solve such problems as hostility, information security, and vulnerability:

1. Hostility : Since we cannot assume that all participants in mobile business are honest, the mobile business system should provide enough mediated and stored information so that dishonest merchants, customers or other players can be found later.

2. Information security : This is a key issue in mobile business. In a transaction, each party involved needs to be able to authenticate its counterparts, to make sure that received messages are not tampered with, to keep the communication content confidential, and to believe that the received messages come from the correct senders.

3. Vulnerability : Data can be lost due to the mobile terminal malfunctions. Worse, these terminals can be stolen and ongoing transactions can be altered.

Some of the above problems seem solvable. Motorola is exploring personal identification numbers for cellular phone security and fingerprint for wireless identification. Some payment methods have been developed to address the secure payment issue in mobile business. The eCyberPay payment solution is such an example. It provides a central contact point for both the Internet and mobile users for accessing services and making payments. It is very user friendly, and does not require credit card information, extra software downloads, or tedious registration procedures or advance payment.

Assessment of Technological threats and Opportunities :

There is a growing realization among companies that technological innovation is a powerful source of competitive advantage. As such, technological innovations present both threats and opportunities not only to companies' short- and medium-term profitability, but also to the longer-term growth and survival. This is true of all technology-based organizations, i.e., those organizations where technology can have an effect on the bottom line in one way or another—and we have yet to be convinced that there is any organization in which this is not the case. There are many examples of companies that were market leaders and financially very strong, but failed or came to serious grief because they misjudged the impact that technological innovations can have on their business [49](Utterback, 1994; and [50]Christensen, 1997). The ability to develop and deploy offensive and defensive innovation strategies has become a necessary element of companies' strategy portfolio, and a framework to assess technological threats and opportunities is an essential component of these strategy.

The framework for assessing technological threats and opportunities that was previously proposed is shown in Fig. 2.3. It follows a two-pronged approach. Firstly, a rapidly changing global technological landscape necessitates keeping track of technological developments. Since the focus here is on innovation (as opposed to mere invention), the market implications are as important as the technological ones and have to be considered as well. One must assess developments not only in the technology field or the market, but rather the interaction in the technology–market domain. Also, although the emphasis is on technological threats and opportunities, social, economic and political issues tend to affect technological diffusion acutely, and hence any methodology for keeping track of technological developments should be able to translate these trends into technological impacts. It is essential to monitor and scan broadly, since industry-shattering and paradigm-shifting innovations very often originate in an entirely different industry than the one that they eventually have the greatest impact on [49](Utterback, 1994).

Secondly, as pointed out above, any organization could be considered to be technology- based to some or other degree, and the second core element of the framework is thus to assess which of the technological developments could potentially impact the organization, typically through a technology or innovation audit. Also, no organization operates in a vacuum, and therefore other entities that interact with the organization in question needs to be identified, be they partners, competitors, suppliers or distributors. Some competitive intelligence practices are thus highly applicable for this activity.

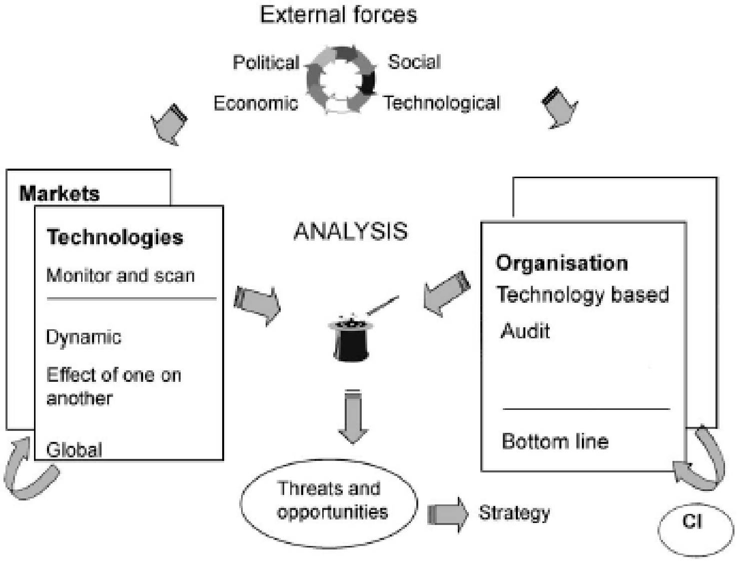


Fig. 2.3 : Technological threat and opportunity assessment [51](Du Preez et al., 2002).

2.2.14. Mobile Communication Devices :

Mobile and wireless technologies are becoming increasingly pervasive. Mobile phones were once considered a luxury, but are now taking the place of conventional telephones in residential use. Wireless networks free users from the tethers that have bound them to their desk, enabling them to live and work more flexible and convenient ways. Historical perspective is presented on the two most widely used mobile communications devices—cell phones and personal digital assistants. Current state, including growth and new developments, of mobile communications is reviewed and a number of industry applications are briefly described. Analysis and ramifications of mobile communications in so far as global business operations are affected providing the concluding thoughts.

1. History of cell phones :

In 1946, AT&T started the first mobile telephone service through the public telephone system. It required a manual search of an open radio channel prior to placing a phone call. The user would link to a mobile operator, who would then dial the call over the public telephone system. In this arrangement, controlled by a talk button, only one party was able to speak at a given time. This was called a “simplex” radio connection [52](Dalglish, 1999). In 1964, Ma Bell improved mobile telephone service. It featured automatic dialing and channel searching with a “duplex” connection. This system had a few channels available as each radio frequency was used only once in the whole geographic region. Usually, in a large city this system could serve about 300 plus customers with another 2000 or more customers waiting for service. In order to provide coverage throughout the entire service area, the antenna for this service had to be placed on a very high structure. Motorola and AT&T developed and introduced advanced mobile phone system (AMPS) in 1983 with over 2 million subscribers of this system by 1988, which was not adequate to cover the demand. In 1991, Motorola came up with an analog system called Narrowband AMPS in which each existing 30 kHz channel was divided into three 10 kHz channels. During same period, late 1980s and early 1990s, Inter Digital Communications Corporation developed and introduced another system, which used digital technology and Time Division Multiple Access (TDMA) method. This approach enabled three new voice channels in place of one AMPS channel. Each subscriber of service could use the entire radio frequency channel to transmit data for shorter time frames. TDMA was designed to operate with the efficiency of digital technology and to create a global standard in which all systems would be compatible. Qualcomm, a San Diego, California company introduced in 1994, another cell phone technology known as Narrowband Code Division Multiple Access (CDMA), which was adopted as standard by the Telecommunications Industry Association. It offered 10–20 times the capacity of existing analog AMPS systems. The rate of growth of worldwide mobile phone sales has been dramatic but has recently tapered off

[53](Standard and Poor's Industry Surveys, 2002). Fig. 2.4 presents the growth of worldwide mobile phone sales on a yearly basis.

Within the United States the wireless industry has grown dramatically. Fig. 2.4 reports yearly growth in the number of subscribers. Along with the growth in subscribers has come a growth in service revenues. Fig. 2.4 presents yearly growth in total service revenues. Why have cell phones been so popular over the last decade? The answer is simple—mobility. The overall dynamics of the industry have changed, with carriers concentrating on profitability rather than raw subscriber growth. In addition, customers had been delaying their orders until new Internet-ready phones were available. On the profitability front, various mobile standards and new technologies have created a more complex production cycle that is increasing manufacturing and research costs. With growth rates for the wireless sector declining, product pricing will become an even more important differentiating factor. Wireless handset vendors that cannot produce in large volumes and gain economies of scale will have difficulty turning profits.

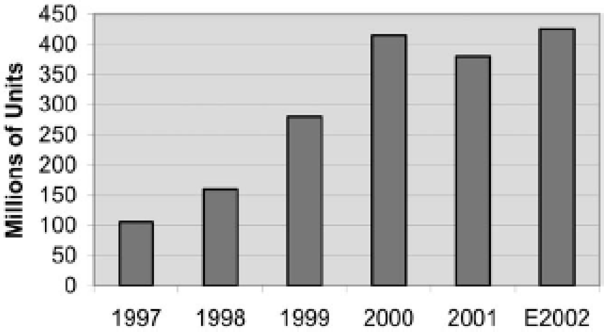


Fig. 1. Worldwide mobile phone sales

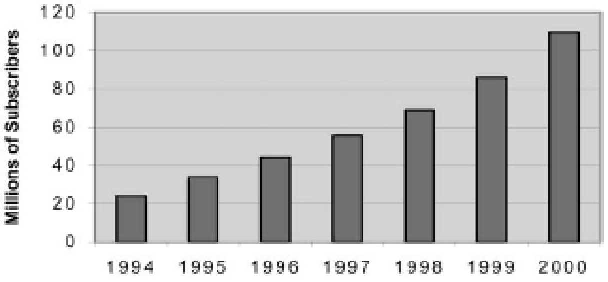


Fig. 2. US wireless industry total subscribers by year

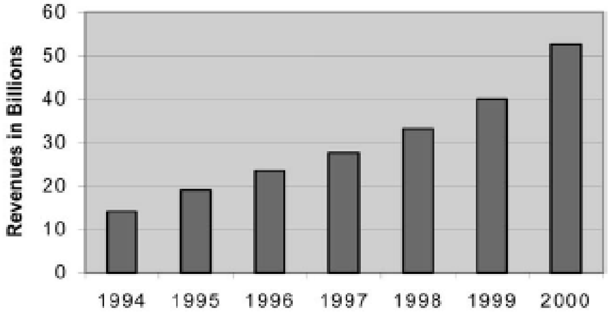


Fig. 3. US wireless industry total service revenues

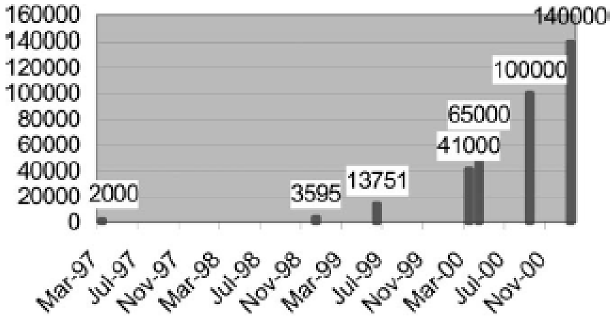


Fig. 4. Number of palm developers

Fig. 2.4 : Growth of worldwide mobile phone sales, number of subscribers etc on a yearly basis (Standard and Poor’s Industry Surveys, 2002[53]).

2. History of Personal Digital Assistants :

The personal digital assistant (PDA) developed from the desire to carry a handheld version of items found on one’s computer, such as addresses and phone numbers, date book, calculator, etc. This topic revolves around Palm, Inc., a pioneer in mobile and wireless Internet solutions and the world leader in handheld computing. It was founded in 1992 [54](Palm, 2002). US Robotics Corporation acquired the company in 1995. In 1996, Palm introduced the Pilot 1000 and Pilot 5000 products that led the resurgence of handheld computing. In June 1997, Palm became a subsidiary of 3Com Corporation when 3Com acquired US Robotics. With its acquisition of Smartcode Technology in February 1999, Palm added advanced wireless communications capabilities to the Palm OS platform to address the market for mobile information appliances, such as cellular telephones, messaging devices, data communicators and smart phones. In June 2000, Palm announced the acquisition of Actual Software Corporation, a leading provider of email solutions for the Palm OS platform and the provider of the award-winning MultiMail line of products. According to 2001 figures, Palm is the leading global provider of handheld computers with a 41.5per cent share of the worldwide personal companion handheld device market, and a

60.3per cent share of the worldwide handheld OS market. Palm products are sold in more than 54 countries and through Internet retail websites.

The Palm Economy—a community of Palm OS licensees, nearly 200,000 registered developers and others committed to advancing the platform and its offerings—has created more than 13,000 software applications and more than 100 add-on devices. Palm handhelds are growing increasingly pervasive as information management becomes ever more mobile. Palm believes that handheld computing is the next wave in individual productivity tools for the global workforce. Developing applications for mobile units to generate revenues is a major undertaking. Fig. 2.4 presents the increase in Palm applications developers since March of 1997 when there were 2000 such developers.

2.3. Mobile Payment Technologies

There are many motivations for both retailers and consumers to adopt mobile payment technology. Compared to the current system that includes credit cards, debit cards and checks, mobile payments will be faster, safer, more widely acceptable, less susceptible to fraud and in the long run will save on costs and increase profitability.

While both sides will benefit from the technology, it will be the retailers that have the most gain and will push for it to be adopted more than the consumer will. Mobile payments have a faster processing time (especially compared to checks), so the retailer gets access to their money faster. The transaction time at the point of sale is also faster, which means that customers can make purchases quickly and long lines will be eliminated [55](Karnouskos and Fraunhofer, 2004). This can lead to more sales, as some sales are lost due to customers not wanting to wait to make a purchase. The new investment and usage cost for mobile payment technology is expected to be low, since the consumers are paying most of the cost when they purchase their own mobile devices. Depending on how privacy laws are defined for this technology, retailers may also be able to obtain more information about their customers. This information will improve their ability to do market analysis, and they also could use customer information to customize service to each customer depending on their purchase history.

Mobile payments will be more resistant to fraud, which is a huge benefit to retailers. In cases of credit card fraud, it is the merchant that ends up paying for most of the losses. The increased security on mobile payments due to added security precautions would greatly increase their profitability. While credit and debit cards already perform most of the payment functions that a mobile device would be able to handle, consumers still have a number of reasons to adopt this new technology due to fraud. It will be very easy for customers to learn to use and gradually will be more widely available to use than credit cards. In fact, it is expected that global standards will be put into place that will allow mobile payments to be accepted worldwide, regardless of where the customers have their accounts.

With mobile payments one will be able to make a payment to anyone else with a compatible mobile device. Finally, the customer will be able to access his/her transaction history easily by viewing it right on the mobile device. In addition to retailers and consumers, other companies can benefit from this new technology. Mobile network operators will grow and increase profits by providing these new services. Mobile device manufacturers will see increased demand and will develop profitable relationships by working with banks and other payment processing providers. When introducing a new form of payment to the public, mass-market acceptance of the new technology is extremely important [56](McMahon et al., 2005; [57]Walker and Barnes, 2005). A large number of retailers and customers have adopted the new technology; otherwise it will fail since few people will use it instead of current payment methods. When credit cards were first introduced in 1951, only a few hundred people had the cards and only a small number of restaurants were willing to accept them.

There are a variety of different technologies that different companies want to standardize handling local transactions. Palm and HP have partnered to develop IrFM (infra-red) technology to allow Palm Pilots to act as a digital wallet. Some US companies such as Verizon, Visa and many Asian companies are also involved with IrFM payment procedures. Many other companies are working on ‘Wireless Wallet’ technology, which requires an always-on connection to the user’s wireless network [58](Chameleon Network, 2003). There are also Radio Frequency Identification-(RFID-) based payment procedures being developed. With RFID, a small chip built into the cover of the phone is scanned, and a Personal Identification Number (PIN) must be entered to authorize the payment. This was developed to be similar to existing credit card technology and to be more able to quickly and easily replace current systems. Some companies have implemented other interesting ways to use mobile devices for transactions. A bank company in Japan allows customers to withdraw money from an Asynchronous Transfer Mode (ATM) by using their mobile phone for identification. Another Japanese company called Telcos has come up with a way to use a mobile device as a form of payment without the retailer having to make any extra efforts to accept mobile payments. A system has been developed that allows a customer at a store to purchase goods with an online transaction, at which point an image of the barcode is sent to the customers’ screen. This bar code can be scanned through an existing optical technology.

Future of Mobile Payment Technology

Because mobile payment is still a new technology that is just beginning to be utilized there is much room for improvement and future technological advancement. The first of these technological advancements, which is being considered, is that of the 3G technologies. Currently all existing systems focus on 2G and 2.5G infrastructures. A few of the approaches to the new 3G technologies were tested with the debut of the Universal Mobile Telecommunications System (UMTS), wireless LAN and WiMAX. With these new systems mobile payment will be freed from some of its current limitations. As the device manufacturers continue to introduce new mobile phones with more sophisticated technology, the idea of advanced cryptographic services will be integrated into the mobile phones, which will allow for a secure voice and data communications. This is an issue that will fix many of the questions of security and privacy. Currently the mobile payment security is very weak. The only reason why this weak security of mobile payment has not been widely exploited is because mobile payment has not become a mainstream medium for payments [59](Young, 2006). Other security technology expected to become available in the future are Mobile PKI, mobile digital signatures, encryption and biometric authentication. Many standardizations efforts are being implemented and mobile payment industry is working towards a federated identity in the virtual world. The security issue that we face in the future is a major obstacle because security was not originally instituted within the networks; security was added later after the vulnerability was noticed. If security standardization is made in the virtual world, this will have a catalytic effect on mobile payment development and the acceptance by the public. This advancement will bridge the gap between the physical world and the virtual world.

Mobile payment is paving the way of the future by rendering the need for paper money obsolete. With the demand for wireless technology growing at such rapid rates it is adding fuel to the fire of mobile payment. With minimal boundaries, mobile payment has a clear shot into the future. Even today new mobile payment infrastructures are being introduced into the world. Many issues still plague mobile payment. The main one is security, but, with the research and standardization being implemented around the world it is in the near future that one’s next purchase will happen with a virtual dollar [60](Herzberg, 2003). These values show that mobile payment reduces the time of a transaction and the cost significantly thus proving to be very beneficial to the economy. It is found that this technology has proven to be very efficient and could be a reliable source of currency in the years to come. With various improvements that are taking place to advance the security of mobile payment, it is in the very near future it is expected to see mobile payments become a widely spread technology and replace paper currency.

2.4. Review of Literature on Online Banking

In India not many studies have been conducted on the current status of online mobile banking. Thus almost no literature is available on this subject in India. There are numerous papers that sought to study the growth of online banking internationally, for instance, [61]Sathye (1997) surveyed the status of Internet banking in Australia. The study found that only two of the 52 banks started Internet banking services at that time. However still there was a lot of room for Internet banking to expand in Australia. Booz Allen and Hamilton Inc. (1997)[62] conducted a global survey covering 386 retail and corporate banking institutions in 42 countries to assess the strategic impact of Internet banking on the financial service industry. According to the study, there is a huge perception gap between North American/European banks and Japanese banks regarding the future of Internet banking. North American and European banks expect Internet banking to become the most important retail channel within 10 years, but Japanese banks expect traditional branches to remain the most important channel. The study also indicates the rapid growth potential of Internet banking. Many of the banks that responded have plans to upgrade the functionality of their Internet service offerings. Egland (1998)[63] conducted the first important study that estimated the number of U.S. banks offering Internet banking and analyzed the structure and performance characteristics of these banks. They have found no evidence of major differences in the performance of the group of banks offering Internet banking activities compared to those that do not offer such services.

Furst et al., (1998)[64] a U.S. based study found out a significant shift by consumers and businesses to electronic payments. In response to developments in electronic payments and remote banking, banks have greatly increased their investment in technology, particularly in retail banking. The gains from technological advancements in banking and payments are likely to be substantial, both from the point of view of individual financial institutions and economy-wide. In this environment, banks should review and, if necessary, adjust their risk management practices in tandem with upgrading their technology activities. Diniz (1998)[65] reported a survey of web sites of banks in USA. It was found that most of the bank websites were basic and intermediate level. No website was found to be of advanced level. Furst et al., (2000)[66] presented data on the number of national banks in U.S. offering Internet banking and the products and services being offered. Only 20 percent of national banks offered Internet banking in the third quarter of 1999. However, as a group, these Internet banks accounted for almost 90 percent of national banking system assets, Banks in all size categories.and 84 percent of small deposit accounts. offering Internet banking tend to rely less on interest-yielding activities and core deposits than do non-Internet banks. Also, Institutions with Internet banking outperformed non- Internet banks in terms of profitability. Sullivan (2000)[67] found that Internet banks in 10^{th} Federal Reserve District incurred higher expenses but also generated higher fee income and concluded that the measures of profitability for Internet banks are similar to those of the non-Internet banks. Guru et al., (2000)[68] examined the various electronic channels utilized by the local Malaysian banks and also accessed the consumers reactions to these delivery channels. It was found that Internet banking was nearly absent in Malaysian banks due to lack of adequate legal framework and security concerns. However over 60 percent of the respondents were having Internet access at home and thus represented a positive indication for PC based and Internet banking in future.

DeYoung (2001a)[69] investigated the performance of Internet-only banks and thrifts in the U.S. The empirical analysis found that the newly chartered Internet-only banks substantially underperform the established banks at first, but these performance gaps systematically diminish over time as new banks grow older and larger. The study suggested that the Internet-only banking model may be feasible when executed efficiently. DeYoung (2001b)[70] found that the average one year old Internet-only bank earned significantly lower profits than the average one year old branching bank, due to low business volumes and high non-interest expenses. It supports the proposition regarding the Internet-only banks, fast growth but low (or no) profits. Jasimuddin (2001)[71] found that within one year of the introduction of Internet service in Saudi Arabia, Saudi banks had at least decided on their Internet presence. 73per cent of the Saudi banks possessed their own web sites and 25per cent of the web sites were offering full services over Internet. The banks viewed the Internet as a key alternative delivery channel. Jathan et al., (2001)[72] conducted the review of Malaysian banking sites and revealed that all domestic banks were having a web presence. Only 4 of the ten major banks were with transactional sites. The remaining sites were at informational level. There are various psychological and behavioral issues as trust, security of Internet transactions, reluctance to change and preference for human interface which appear to impede the growth of Internet banking. Furst et al., (2002)[73] provided a comparative study of Internet and non-Internet banks in U.S. and found that institutions with Internet banking outperformed non-Internet banks in profitability. Also, banks in all categories of size offering Internet banking tended to rely less on interest yielding activities and deposits than non-Internet banks do.

Koedrabruen et al., (2002)[74] investigated, designed and developed an Internet based retail banking prototype that meets the requirements of the Thai customers. It found that more than half of the sample Internet users in Thailand are very interested in using the Internet banking services. The main features needed are balance inquiry, bill payment, fund transfer, business information, and payment for goods purchased. The prototype was then developed and validated. The survey from the executives of four Thai banks revealed that there was a potential growth for retail Internet banking in Thailand. Corrocher (2002)[75] investigated the determinants of the adoption of Internet technology for the provision of banking services in the Italian context and also studied the relationship between the Internet banking and the traditional banking activity, in order to understand if these two systems of financial services delivery are perceived as substitutes or complements by the banks. From the results of the empirical analysis, banks seem to perceive Internet banking as a substitute for the existing branching structure, although there is also some evidence that banks providing innovative financial services are more inclined to adopt the innovation than traditional banks. Hasan (2002)[76] found that online home banking has emerged as a significant strategy for banks to attract customers. Almost 75 percent of the Italian banks have adopted some form of Internet banking during the period 1993-2000. It also found that the higher likelihood of adopting active Internet banking activities is by larger banks, banks with higher involvement in off-balance sheet activities, past performance and higher branching network. Janice et al., (2002)[77] based on interviews with four banks in Hong Kong noted that banks view the Internet as being a supplementary distribution channel for their products and services in addition to other forms of distribution channels such as Automated Teller Machines (ATMs), phones, mobile phones and bank branches. Basic transactions and securities trading are the most popular types of operations that customers carry out in Internet banking. Lustsik (2003)[78] based on the survey of experts of e-banking in Estonian banks found that Estonia has achieved significant success in implementation of e-banking and also on the top of the list in emerging countries. All the major banks are developing e-business as one of the core strategies for future development.

Awamleh et al., (2003)[79] found that banks in Jordan are not fully utilizing concepts and applications of web banking. In comparison to developed international markets, it is fair to say that this sector is largely undeveloped. Indeed, only two banks offered limited number of services through their web. The major challenge facing further development of web banking in Jordan is, for example, the high cost of telecommunication. Another element is the non-availability of information technologies, packages, solutions, and human resources, which facilitates optimum use of technology. The study revealed that Jordanian banks have been successful in the introductory phase of web banking. However Jordanian banks are required to move towards web banking usage with a view to conducting real financial transactions and improving electronic customer relations. Mari Suoranta et al., (2003)[80] focused on studying diffusion and adopters of mobile banking services. The paper explores some contradictory empirical findings drawn from a mobile banking survey. The results provide an indication of the characteristics of potential subsequent adopters of mobile banking, and of differences between user segments. It also commented on the influence of certain demographic characteristics and the preferred communication mode of customers on the adoption and future usage of mobile banking services. Jukka Riivari, (2005)[81] looks at how and why financial organisations across Europe are beginning to take advantage of mobile services and in particular mobile banking as a powerful new marketing tool to build long-lasting and mutually rewarding relationships with new and existing customers. Examples show how European financial organisations are using mobile banking to improve their customer service and relationships, to reinforce their brand by literally placing it in their customer's pocket and to reduce their costs. Mari Suoranta et al., (2005)[82] reviews recent technological advances in banking and forces that will drive or inhibit mobile banking services adoption. Drawing on the relevant literature and empirical implications of the study, the paper proposes a model that conceptualizes different affecting factors in electronic banking environment, and particularly in mobile banking. A quantitative survey sheds more light on this researched issue. The data was collected in Finland during May–July 2002. Irwin et al., (2005)[83] explored the factors that affect Internet and Cell Phone banking adoption in South Africa. The paper also compare the differences in the perception of Internet banking and cell phone banking and the influence factors. The findings indicate that both the adoption intent and the perception of Internet banking users differ markedly from cell phone banking users. The exploratory study of Vijayan et al., (2005)[84] seeks to examine the consumers' intention to adopt themselves to multimedia banking based on three commonly used theories known as Technology Acceptance Theories (TAT). Even though multimedia banking is well available in the market banks are generally facing immense challenges in attracting visitors to their websites. As much of these phenomena were blamed on the traditional brick and mortar type of banking, knowledge and understanding of this challenge can help bankers to fish in more clients into this new wave of banking. At the same time to stay competitive in the market banks have to develop a framework that incorporates latest technological aspects of multimedia banking.

In the Indian context many publications throw light over the importance of Internet banking and also its prospects for the Indian banking industry. However these papers don't identify key differences between Internet banks and non-Internet banks. Unnithan et al., (2001)[85] studied the drivers for change in the evolution of the banking sector, and the move towards electronic banking by focusing on two economies Australia and India. The paper found that Australia is a country with Internet ready infrastructure as far as telecommunication, secure protocols, PC penetration and consumers literacy is concerned. India, by comparison, is overwhelmed by weak infrastructure, low PC penetration, developing security protocols and consumer reluctance in rural sector. Although many major banks have started offering Internet banking services, the slow pace will continue until the critical mass is achieved for PC, Internet connections and telephones. However, the upsurge of IT professionals with growing demands is pressuring the government and bureaucracy in the country to support and develop new initiatives for a faster spread of Internet Banking. The economy is classically the catch-up one, trying to develop and catch up with leading economies. Rao et al., (2003)[86] provided a theoretical analysis of Internet banking in India and found that as compared to banks abroad, Indian banks offering online services still have a long way to go. For online banking to reach a critical mass, there has to be sufficient number of users and the sufficient infrastructure in place. Agarwal et al., (2003)[87] explored the role of e-banking in e-democracy. With the development of asynchronous technologies and secured electronic transaction technologies, more banks and departments were using Internet for transactional and information medium. Initiatives such as E-SEVA and FSC’s are the milestones towards achieving comprehensive e-governance. Balwinder Singh et al., (2004)[88] made a survey of commercial banks websites, on the number of commercial banks that offer Internet banking in India and on the products and services they offer. It investigates the profile of commercial banks that offer Internet banking, using univariate statistical analysis, relative to other commercial banks with respect to profitability, cost efficiency, and other characteristics. By the end of first quarter, 2004, differences between Internet and non-Internet banks had begun to emerge in funding, in sources of income and expenditures and in measures of performance. It was also found that the profitability and offering of Internet banking does not have any significant correlation. Sakkthivel, (2006)[89], conducted an extensive primary research in Bangalore, India (Silicon Valley of India) in order to identify the willingness of Internet users to buy different services over Internet. The paper aims at providing a specific focus to identify the impact of demographics in influencing Indian Internet users in consuming different services online. The outcomes would help the corporate world to understand the importance of demographics on online purchase which could be adopted and deployed for better use. Internet banking is fast becoming popular in India. However, it is still in its evolutionary stage. By the year 2005, a large sophisticated and highly competitive Internet banking market will develop. Almost all the banks operating in India are having their websites but only a few banks provide transactional Internet banking (Mookerji, 1998 [90]; Pegu, 2000[91]; and Dasgupta, 2002)[92].

2.5. Significance of Mobile Business in Financial Sector

2.5.1. Penetration of Mobile Usage in India :

In India, the growth of mobile plateaus is at around 13,00,000 new subscribers every month. India had 14.17 million mobile phone subscribers by May 2003, about 102.8 percent more than the year

2003 and as of end October 2004, the total number of mobile subscribers in the country was 44.51 million as compared to 43.96 million fixed line subscribers. It is also noted that the GSM industry continued to maintain its dominance in the mobile market accounting for 78per cent of India's total mobile subscribers. Mobile phone users are grown to over 160 million by the end of the year 2006 and 220 million by the end of the year 2007. This is due to the following seven reasons :

Essentiality of mobile device rather than luxurious :

The tight emotional attachment with the family members and friends, Indian citizens like to keep continuous contact with each other at any where any time. This attitude of Indian people is supported by the advent of less cost mobile communication technology and becoming popular in upper as well as middle class people.

Continuously decreased price of mobile devices :

The price of mobile devices is continuously decreasing year by year and is now affordable to common people in India. In addition, the technology of mobile device is improving such as increase in screen size, improved bandwidth and internet accessibility.

Low usage cost :

Due to high competition between mobile service providers and globalization of business, the cost per call is very small and is further decreasing substantially.

Availability of services in rural areas :

Due to decreased cost of mobile equipments and communication services, rural people also attracted towards the usage of mobile services. Moreover, the competition between mobile service providers and hence decreased usage cost also attracted the middle class people in rural areas. Also, the additional bundled services like mobile banking, internet access facility using mobile device and mobile commerce attracted educated people in rural area which caused further penetration of mobile usage in India.

Integration of various service applications within a device :

The bundling of various additional services like, video camera, free SMS, broad band Internet access facility at nominal charges, Downloading video games, weather report, Alarm, date and time, calculator, hot news, online banking facilities, online purchasing of various products and services attracting people to use mobile devices and services.

Improved willingness to use mobile devices :

The attitude of the people towards the usage of mobile devices for their daily applications is changing and the willingness of the people especially youngsters towards usage of mobile devices is increasing. More and more people in urban and rural places are attracted to the advantages of mobile communication technology and willing to use them in their daily life.

Improved economic conditions of the people :

Such an extremely high penetration rate of mobile devices, especially mobile phones coincidences applications other than communication between people, which include mobile financial applications such as mobile banking and mobile payments. This is also due to the fact that users considered their mobile phone as a personal trusted device making it to an integral part of their lives and more and more of these devices became Internet-enabled, which is suitable for banking applications. Cellphone firms in India get ready to harvest the high growth potential of mobile phone market. With subscriber addition drying up in older cellphone markets in Western Europe and North America, the bigger players in the mobile phone industry are turning to emerging markets – India and China to keep growth rates high. World leaders Nokia and Motorola, who accounts for more than 51per cent of the phones sold in the World today, continue to bring out cheaper and cheaper models in the market with basic features like voice, SMS and mobile banking at around Rs. 1000. Another player, Philips, less dominant in handset market but which accounts for almost 15per cent of the chipset business has also a plan to bring out Cellphones under Rs. 1000.

The Indian Government has given unstinting support to the telecom sector, which is a critical infrastructure for economic growth of the country and has a direct multiplier effect on the economic growth. Responding to the support, the Indian cellular industry has put in a significant performance in the recent past. Today, the number of mobile subscribers has exceeded the number of fixed line subscribers and is continuing to grow appreciably. The Telcom industry has invested over Rs. 60,000 crores in setting up 150 state-of-the-art cellular mobile networks serving about 4,000 cities/towns and over 60,000 villages all over the country. The Cellular service providers are offering world-class digital mobile services to the consumers at the most affordable tariffs in the world.

2.6. Services in Online Mobile Banking

Basic online banking covers the account management via electronic devices. However, type of mobile banking services are classified in three types as : Information services, communication services and transaction services. The information service provides the information about various products and services available for the customers. This level of banking service can be provided on a stand-alone server by the bank itself or by sourcing it out. Since, the server or Website may be vulnerable to alteration, appropriate controls must therefore be in place to prevent unauthorized alterations to data in the server or website. The communication level allows interaction between bank's system and the customer. This types of services may be limited to account inquiry, loan applications, request for cheque book, an e-mail to stop account transfer, static file updates etc.

Under this kind of services, the customer makes a request to which the bank subsequently responds. In communication service, the risk of any unauthorized attempt to access to banks internal network and computer system is more compared to information service. The transaction level allows customers to execute transactions like accessing and fund transfer between accounts, paying utility bills etc. These services require higher level of risk and must have strongest controls which demand very stringent security.

The online services generally offered by Indian banks are :

Account balance/statement: After logging in, one could check his account balance and view a list of recent transactions, view an account statement online and print it if needed. Citibank also lets to view the relationship summary and loan account statement online.

Electronic transfers: Enables the customer to transfer money between two accounts in the same bank. Some banks provide a facility for transferring money between NRI (Non-Resident Indian) and local accounts.

Bill and loan payments: Banks offering this facility to receive, review and pay customers bills or loans online. Besides loan payment, one can opt to pay electricity, water, phone, credit card and cellular phone/pager bills, through the bank. Once the customer confirm the transaction, the payment will be automatically made. Some banks also provide schedule payments for a future date.

Credit Cards: Using this facility, the customer can access details about his credit card statements, payment status and requests. Citibank allows its customers to increase his credit limit online, or apply for a second credit card.

Requests: This facility allows to request a new cheque book, some deposit slips or a demand draft. It also allows to issue a stop-payment instruction using a mobile device. The cheque book, deposit slips and draft will be delivered by courier.

Information: Mobile banking can also provide information at customers fingertips. For instance, one can view forex rates or interest rates.

E-mail: Some mobile online banks offer an e-mail facility. This is used exclusively for sending queries to a bank executive. Although an e-mail response from the bank may not be as instantaneous as telephonic help, it does help in providing specific information.

Investment services: This includes online transactions for stocks and shares and investments like mutual funds and demat.

Miscellaneous services: Online banking facility also allows to inform lost cheque, stop payments, lost ATM card or credit card, to the bank, and expect some immediate action.

E-commerce: Online banks are setting up their own payment gateways and are preparing to become payment facilitators for B2C e-commerce transactions. HDFC and ICICI Banks have already set up a payment gateway for facilitating payments for goods.

Table 2.1 : Push or Alert and Pull or Request Facilities available in Indian Banks :

Type of Mobile banking service	Facilities
Push or Alert	All significant transactions alert Cheque bounce alert Cheque paid alert Clearing cheque deposited/regularized alert Maturing and matured term deposit alert Standing instructions to operating account Nearest bank branch location Balance in Account falls below certain amount. Credit of salary into account . Loan installment overdue . Locker rent overdue . Suspending self from SMS alerts
Pull or Request	Account balance Last 3/5 transaction details Cheque book request Enquire cheque status Stop cheque payment Account statement Registration for SMS banking Fixed deposit details Pay your utility bills . Bill presentment . Fund transfer between own accounts . Renew term deposits . Set operative account

	. Change your primary account . Debit card reward points . Help facilities . Details of balance in Credit card . Reward points available . Credit card details of last payment . Credit card payment due date . Demat status enquiry . Demat status of transaction . Information related to loan . Nearest bank branches . Nearest ATM location . List of banks under ATM sharing . Latest deposit interest rate . Change SMS password . Cancel Registration of SMS banking . Domestic/NRE/FCNR deposit interest rate . IFSC code and name of the bank branch . Applying for new PIN . Mobile phone recharge

2.7 Review on Security Issues on mobile banking Transactions :

Security is a business issue. Technology solutions, key business principles and strong management commitment play a critical role in establishing a rigorous framework for sound risk management and robust security practices. Information security is fundamental to the reputation of the business and its underlying operations. The ability to develop and maintain market and customer confidence is contingent upon the adequacy and reliability of security practices. The effectiveness of security risk management is predicated on the ability to identify threats and vulnerabilities and the resultant actions taken to reduce their potency and potential impact to an acceptable level. Customer trust in banking and payment services, including the technologies deployed, is fundamental to the safety and soundness of the financial industry. In a Mobile Security, Jain (2006)[93] makes a salient point: “The vulnerability of mobile computing and communications is a big but sometimes hidden enterprise security threat. Mobile handhelds are compact, portable and easily lost or stolen, and hence, put sensitive information at risk. The proliferation of insecure WLAN networks pose a further threat to corporate security.” In order to keep a mobile banking system secure, Tang, Terziyan, and Veijalainen[94] outline five security requirements:

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authorization

Confidentiality ensures that non-public information remains private. Confidentiality through mobile devices is challenging because these systems depend on wireless communications and generally use the Internet. Authentication is the process of identifying a user to be who they claim to be. This usually takes the form of a credential (e.g., username and password). Integrity ensures that data is not tampered with on its path to its destination. This is concerned with preventing man-in-the middle attacks or other active session hijacking attacks. Non-repudiation ensures transactions are legally binding. This is critical for electronic banking systems because it prevents complication from regulation violation. Authorization ensures transactions are endorsed and authorized by all parties involved. This comes into play with inter and intra bank funds transfers. (Tang, Terziyan, & Veijalainen, 2008)[94]. In the next section we will look at a number of security topics as they relate to these requirements and to the mobile banking platforms already discussed. This overview will allow us to identify areas of risk and some possible solutions.

2.7.1 Authentication

All mobile banking systems need to use at least two separate forms of authentication to identify the customer. (“Authentication in an Internet Banking Environment”) There are three forms of identification: what you have, what you know, and what you are. What you know includes items like usernames, passwords or pin numbers. What you have examples include a debit card, a smart card, or your mobile device. Who you are requires biometrics (Clarke, 2005)[95] Current authentication methods available include a PIN number for the phones and a PIN number, one-time password or pin number, or a username or password for the banking systems. PIN numbers, usernames and passwords depend on what the user knows, and the literature includes well documented flaws of this model, such as users using weak, guessable, passwords, users writing them down, leaving them where they are found, or sharing them. A survey conducted by Clarke and Furnell (2005)[95] found that 66% of those surveyed used a PIN on device startup, but 30% thought PINs were inconvenient. Additionally 38% had their mobile devices unlocked by their service provider because they had locked themselves out. One solution has been proposed to help protect mobile devices by increasing the security of the PIN itself. When PIN protection is enabled on a mobile device that device only stores a portion of the PIN. The other portion of the PIN is stored on a server. This distributes the PIN in such a way that even if an attacker has direct access to the phone they can only get half the PIN from the phones' memory. Mobile banking systems currently utilize this concept in part. The bank provides the PIN and authenticates it through the phone. 3G network technology will help bring about changes and the increased functionality of mobile devices make it possible to use additional and more advanced authentication methods. (Clarke, 2005)[95]. The system currently used by Wells Fargo for SMS messages currently relies on the phone number are the primary means of authentication. The phone itself is perhaps not the greatest authentication tool we could use. It has some advantages like the fact that the user must have the phone to utilize these services and only this one phone can use these services. The problem becomes the bank can't tell if it's a real customer not. Another form of authentication is "What the user is". Essentially this is the use of biometrics. In a 2005 survey, Clarke and Furnell found that 83% were in favor of using some type of biometric system to protect their phones, including one of the five listed below:

- Facial Recognition
- Keystroke Analysis
- Handwriting Recognition
- Speaker/Voice Recognition
- Service Utilization

A biometric authentication method that deserves note is service utilization, where users are granted or denied access based on their previous behavior and utilization of certain systems. Behavioral analysis looks for patterns of how users do certain things. For example, if a user has to transfer funds, there are several different ways a user can access the transfer portion of the application. Different users may use different ways to access that portion of the system. The way this can be utilized for authentication is if they suddenly do things a different way, it raises a red flag (Mazhelis, 2007)[96]. The technology to fully utilize service utilization is only partially in place; however, service utilization holds promise in the near future. Another authentication technique is out-of band communication, which allows the bank to identify the customer through a communication channel other than the one being used (Feig, 2007)[97]. Bank of America utilizes this method with their mobile banking system. Customer gain access to the system by visiting www.ba.mobi and entering their username/password. Bank of America then sends the customer a pin number as a text message, which is then entered to gain access to the system. A robust authentication system utilizes multiple forms of identity at application startup and during application use. While using an application, the system may test behavior or compare keystrokes to patterns which are on file. If an anomaly is detected, the system could prompt for a more intrusive but more accurate form of identification. If the user fails again, an IVR system could call and use voiceprint analysis along with a PIN. Eventually, if the user fails enough they are locked out. This approach promotes increased security as it is difficult for an attacker to keep getting the right answers (Clarke, 2005)[98]. There are a number of possibilities for authentication across mobile banking architectures. SMS systems utilize tokens and could also utilize tokens in the form of smart card in order to take authentication off one device and provide different options for the user to move around. SMS systems can also utilize PINs by having the user send a PIN or by utilizing an IVR system to call the user to verify the PIN. These systems can also benefit from the use of 1 time PINs at system startup and when questionable activity is detected. Mobile web systems mainly utilize user names and passwords; however, some mobile web services also use out-of-band authentication because they utilize 1 time passwords sent in the form of an SMS message which must be entered into the webpage to log in. This feature promotes good security because an attacker can’t just try to log into the site as they also need access to the phone to get the password. Client side applications benefit from their ability to be highly customizable, often utilize usernames and passwords, PIN numbers, or out-of-band authentication.

2.7.2 Denial of service

Denial-of-service (DOS) is the process of preventing access to a device or system by overwhelming it with phony communication, therefore rendering it unable to accept legitimate transactions. DOS attacks are prominent in wired networks and are making their way into wireless/mobile solutions. It is possible to use several mobile devices to send a stream of SMS messages to another mobile device. This type of attack is called a SMS flood and sends thousands of messages anonymously in seconds (Jain, 2006)[93]. ClairMail (2007)[98] states that a limiting factor in launching a DOS against a mobile banking platform is the cost of attack. Carriers charge to both send and receive information. It’s possible that the next slammer will utilize SMS messages and could cripple a company if it is not detected. The mobile web and client application architectures are vulnerable to a traditional DOS attack. For example an attacker could use a DOS to knock a user’s phone offline with an SMS storm then try to connect to their banks mobile website while the victim’s phone is disabled and incapable of receiving any alerts or messages from the bank. Mobile banking systems are vulnerable to both existing types of DOS attacks and those that can be launched though new delivery channels like a SMS messages. If an attacker were to launch a sustained DOS against a banks mobile website for example it would be very costly to the bank both financially and could have a negative effect on their customer relationship. An attack such on the banks SMS system could limit customer accessibility by both SMS users and java based applications and could have a more damaging financial affect because the bank may be charged for receiving the messages.

2.7.3 Lost and Stolen Phone

Cell phones are small and portable; however, the disadvantage is that they are easily lost or stolen. When considering the threats of lost or stolen devices there are three different areas of note: authentication, authorization, and confidentiality. The threat of this is real with 1.3 million devices being lost or stolen in the UK in 2001 (Clarke, 2007b)[99]. This threat increases as the number of phones increases and, in 2006, over 1 billion phones were sold worldwide, with 80 million of them being smartphones(Lin 2007)[100]. The use of smartphones is growing by an estimated 70 percent in that same timeframe (MacLeod, 2006)[101]. Smartphones are at greater risk not only due to their growing numbers but the fact that they can store an entire identity. A 2007 survey found that 44% of users didn't use a PIN(Clarke, 2007b)[99]. Since users can't be counted on to secure their devices and the software on them other approaches must be found. Two actions are available if a mobile device is lost or stolen. The bank can disable a user's mobile banking services just like they can with a lost or stolen debit card. Second, AT&T ("AT&T Mobile Banking") and ClairMail incorporate features that prevent their system from responding back to a compromised phone. CellTrust also provides the ability to use a phone and remove information from a compromised device as long as it is connected to a network. The CellTrust system has the ability connect to the phone to remove the banking application if a phone is compromised.

2.7.4 Phishing, Vishing or Smishing

Social engineering attacks are dangerous because they exploit human error. Phishing, vishing, and SMiShing are all attacks used to get users to give up their authentication information so an attacker can gain access to their accounts by appearing to be a legitimate user. Phishing is the practice of luring unsuspecting users to a fake website by using authentic-looking email with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack.

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public. SMiShing uses SMS messages instead of voice communication to get the information from the victim. Most of these attacks are launched from an email pretending to be someone the user knows telling them to verify information, and then redirects them to a fake website to have them fill out a form the attacker can then use to steal their credentials or worse their identity. Mobile devices are at risk from this threat, especially SMiShing. Instead of an email, an attacker could send a text message and make it look as if it's coming from the bank, saying "We need you to call 1 800 123 4567 and talk to the representative and verify your account information." IP-enabled phones are just as vulnerable to an attack as a traditional computer. Just send an email with a link to a mobile website and have then fill out the form and the attacker wins. Since mobile banking commonly uses traditional authentication methods such as a user name and password if an attacker can fool the user into releasing their credentials that users information and identity are compromised and this could lead to serious financial loss to banks as well.

2.7.5 Phone Cracking and Cloning

Cracking is defined as to break or snap apart. Attackers find ways to "break" software to gain control of a device. Cloning is defined as making multiple identical copies of something. Cloning mobile devices is duplicating same identifying information as the original device on a phony device. Cracking and cloning threaten authentication and integrity. If a phone is cracked an attacker gains access to data stored on the device. An example of a phone crack on the I-Phone was done by ISE, which deployed an attack called fuzzing to inject invalid data into a program looking for a buffer overflow. They found an exploit in the I-Phones web browser to gain administrative privileges of the phone. Subsequently, an attacker could view SMS message logs, call history, and have data sent back to their machine(Miller, 2007)[102]. Another known phone crack exploits vulnerabilities in Bluetooth. If a phone is Bluetooth enabled, any Bluetooth device within 30 feet can connect to it (Lin 2007)[100]. Using a technique known as Bluesnarfing, an attacker remotely downloads, uploads, or edits files on a device within range without the owner's permission. One test of this in London with 943 phones found 379 had their default settings on and 138 were vulnerable to the attack (Goodwin, 2005)[103]. Cloning new cell phones is difficult, while older analog phones were relatively easy to clone with some basic radio reception equipment. To defeat digital phones however takes a lot more effort and an attack requires sophisticated electronics to clone a GSM phone. To clone CDMA phones an attacker simply needs to get the phones electronic serial number (ESN) and mobile identification number (MIN) (Lin 2007)[100]. One Alltel customer from Wisconsin had her phone cloned and over 100 calls made after she visited a small town near the US Mexico border. Another Alltel customer from Ohio experienced the same problem after a trip to Florida. The problem affects all carriers and every phone is subject to cloning if it is left on. An attacker can use a device to scan for the signals sent out by the phone and can obtain the codes used to identify the phone. An attacker can get all the components required to build a cloning device from any electronics store for less than $2000 and can build a device sophisticated enough to capture phone signals from up to a mile away (Vandini, 2008)[104]. In terms of mobile banking we must consider both cracking and cloning as active threats. Cracking is a threat because an attacker could pull sensitive data off the phone. They could also use cracks to install malware. Cloning is a great threat because an attacker could fake the phones information and possibly have half of what is needed to identify a customer. An attacker could also use cloning in conjunction with a DOS to access the users data without their knowledge.

2.7.6 Questionable Activity

Questionable activity is concerned with authorization, authentication, and nonrepudiation. For example, if a customer only occasionally checks the balance of one or two accounts using their mobile device and on occasion transfers small amounts between his own accounts, then this is their typical behavior. If one day this user requests a large funds transfer to a third party account or a bill pay payment to someone they have never sent funds to before, this is questionable activity, disallowed and flagged for follow-up. If a transaction is questionable but we have determined that the user is the legitimate user we must ensure that the transaction is legally binding so an user can’t come back later and claim that it wasn’t them. Credit and debit card companies today use a variety of techniques to monitor the normal activity cards and similar behavioral based detection systems can be used with mobile banking platforms (Mazhelis, 2007)[96]. Several currently deployed banking systems, like those of ClairMail, have questionable activity monitoring capabilities. An example can be found in the online banking systems, like the one used by Bank of America, an unusual transaction will trigger the bank to send a text message containing a 6-digit pin to a customer’s phone. The bank sends a message to the customer telling them that they will be getting a call from the banks outbound IVR asking for PIN verification. The bank then calls the phone number on file for the customer and asks to verify the PIN before completing the transaction. For added security a bank could also use a voice authentication system to not only verify the PIN but the customers voice as well(Feig, 2007)[97]. Questionable access to some resources may also want to be examined. For example, if the user was just using their services in Chicago and an hour later is trying to connect from Hong Kong that should through up a red flag. Systems need to be able to detect and respond to these threats in a user friendly manner.

2.7.7 Sensitive data, Signatures, and Encryption

Another aspect of a mobile banking system is how it deals with customer data that must be kept private. A system must ensure that regardless of where the data is stored an attacker can’t read or manipulate the data. Solutions like signatures provide non-repudiation. When it comes to existing mobile banking systems, the two most commonly used systems, being Mobile Web and SMS, store most of the sensitive information on a bank’s server. Mobile web applications require the mobile device to connect to the bank's web server, where all the information is stored and processed. Again, the use of account nicknames and limited access to account information affords more protection when attacker tries to compromise an account. Client applications are what present the real threat to data integrity. These applications can utilize account nicknames to help protect account numbers; however, most of the processing is done on the mobile device. There are solutions to protect the data on the phone: 1) encrypt the information stored on mobile devices, 2) encrypt the communication so that if an attacker is able to intercept the message it's still useless without the key. The currently accepted standard of encryption is the highly secure Advanced Encryption Standard (AES).

CellTrust utilizes AES in conjunction with special micro clients to protect SMS messages and gives the ability to send SMS messages containing encrypted messages. The phone can then decrypt the messages for the end user. ClairMail also points to the use of SSL and HTTPS during message-data communication. They also store information such as mobile profiles in Blowfish Encryption Algorithm. However, there is no encryption technique specifically designed for mobile devices. Mobile devices generally lack processing power to encrypt/decrypt efficiently. Yuh-Min Tseng (2007)[105] proposes a group key protocol for mobile devices. Many current security techniques for wired networks don't function as well on low-power mobile devices and their wireless networks. Also another tool that can help with end-to-end encryption and protection of mobile devices are TPM's designed specifically to work on mobile devices or security smartcards. These devices are chips that are added into the motherboard and add the ability to store keys, signatures, passwords, and digital certificates. These devices will aid in the storage and processing of various security procedures and can help improve overall device security. The real advantage to these is they allow for seamless, cost effective, and transparent to the users, which gives greater chance of being used (Berger, 2007)[106]. The OS and digital signatures can also play a role in the encryption process as well. For example, Windows mobile offers the ability to create and store keys, manage certificates and run cryptographic operations. Symbain also has modules that can aid in key and certificate management as well. The features of an OS can be further enhanced by the use of smart cards designed to aid in key management and signatures and certificate storage. Digital signatures offer the customer the ability to sign documents without needing to visit a branch. In e-commerce security systems, non-repudiation is used to provide evidence that a party participated in a transaction. This concept can be used in m-banking as well. For example, signatures can be used to ensure that the customer did authorize a bill pay payment before it's sent. (Ruiz- Martínez, et.al.,2007)[107].

2.7.8 Viruses and Malware

While PC viruses outnumber mobile device viruses, it is easier for mobile device viruses to propagate. As adoption of mobile banking systems increases, so will the attacks on mobile banking systems. The world of mobile devices has already caught the eyes of several attackers and a number of proof of- concept viruses have already emerged. (virus wars) Those devices running Microsoft's Windows Mobile are of particular concern given anything Microsoft tends to be a favorite target of the hacker community (Malykhina, 2006)[108]. A number of mobile viruses are currently a threat to mobile devices. Commwarrior uses MMS and Bluetooth to spread malware from device to device(Lin, 2007)[100]. Wesber and Redbrowser are similar viruses that infect windows devices and send SMS messages(Malykhina, 2006)[108]. These viruses mainly test spreading mechanisms but others are capable of delivering a dangerous payload. The Skulls Trojan infects Symbain devices and overwrites and corrupts applications. Bluetooth is the most common spreading mechanism used by viruses. This is because many newer smartphones are coming Bluetooth-enabled and any Bluetooth enabled device within range can be infected. This was demonstrated in Finland when a minor outbreak of mobile-malware spread from Bluetooth device to Bluetooth device at a soccer game(Conry-Murry, 2005)[109]. Another example of the threat Bluetooth can represent is business men and women beaming electronic business cards to each other. It is possible for an attacker to put a virus into his or her card that could be uploaded into a competitor's network for some sort of personal or financial gain (Jain, 2006)[93]. Bluetooth isn't the only spreading mechanism though. Attackers have written malware that uses both the internet and cellular networks to spread. Additionally SMS and MMS can be used to spread messages containing Symbian Installation System (SIS)(Conry-Murry, 2005)[109]. This threat can be a major concern to both banks and end users. They can be used to launch a number of attacks against mobile banking systems from message flooding of the banks systems to the installation of malware to obtain user credentials or account information. Antivirus companies like Symantec have produced mobile anti-virus tools to help protect mobile devices. Symantec now offers a mobile antivirus designed to protect Windows mobile devices (Malykhina, 2006)[108]. Symantec has been working for several years with Nokia and now, Nokia has Symantec software on their Series 60 smartphones. This software is capable of passively scanning for malware in SMS, EMS, MMS, HTTP and e-mail files and can also be ran manually (Saran, 2005)[110].

2.7.9 Traffic Intercepts

Active wiretapping or traffic intercepts attacks are concerned with intercepting and/or altering the data while it is in transit (Schneider, 2007)[111]. This is also known as a man-in-the-middle attack (MITM). Essentially, an attacker intercepts information sent through communication channels and alters that information, which is a threat to the integrity and confidentiality. Another data integrity threat is a replay attack, where the attacker watches a transaction while the user completes it but doesn’t actively get involved at the time. Instead the attacker merely gathers information and at a later time duplicates user activity to get the desired result. Mobile banking systems must consider the security threats that are raised by traffic intercept attacks. This threat is increased if the user connects via a wireless hotspot and instead going through the more tightly controlled network. Since we are dealing with IP enabled devices without firewalls they could become easy victims. The best way to protect data in transit is with the use of encryption. A system deployed by CellTrust includes encryption in SMS messages that utilize micro clients to enable encryption of messages and send several messages that the clients can decrypt.

2.8 Review on mobile payment

A variety of mobile technologies and mobile services have emerged during the last two decades. The term M-Commerce was adopted by marketers in the late 1990s, and predictions were made of rapid growth in the volume of commerce conducted through mobile devices. By 2004, Jupiter Research had become vastly more optimistic, offering "Global mCommerce Revenue Projections for 2009" of $426 billion, most of it in "phone-based retail POS sales" ePayNews.com (2002)[112]. On the other hand, the slow growth had led other organisations to offer much more circumspect prognostications, e.g. "2006 will continue to see the development of experiential mobile applications and the emergence of m-commerce services, increasing in reach and importance over the next two years" (Atos 2005, p. 12)[113]. Juniper Research remains unabashed, and was quoted in early 2008 as forecasting that "over 612 million mobile phone users would generate over $US587 billion ... worth of financial transactions by 2011" (Moses 2008)[114].

Despite one or two consultancy groups' wild enthusiasm, the growth of M-Commerce has a very patchy record. One major concern is that the risk of financial loss acts as an impediment to the adoption of mobile commerce. This may be because of widespread knowledge of actual losses, or reports of vulnerabilities, or just from uninformed concerns and natural risk-aversion. In order to understand the substance of the issue, and to avoid unnecessary delays in mobile service adoption, it is highly advisable that payment schemes intended for use in mobile contexts be subjected to risk assessment. As with any form of trading, M-Commerce involves multiple steps, including partner discovery, information exchange, negotiation, contracting, delivery and settlement. The settlement step necessitates considerably greater care than the others, because the payments process creates considerable opportunities for funds to be stolen, with low likelihood of the thief being apprehended or the proceeds recovered, and with the possibility that the victim may not even be aware that the theft has occurred.

The term 'mobile payments' is used to refer to any payment that is conducted by means of a mobile access device and wireless network connection. By 'mobile access device' is meant 'any device that provides users with the capacity to participate in transactions with adjacent and remote devices by wireless means'. Such devices comprise at least a processor, systems software, application software and wireless communications capability. They are commonly also capable of at least some forms of physical interaction with one or more storage devices such as magnetic disks, CDs, DVDs, and solid-state tools (e.g. 'thumb drives' or 'memory sticks' or, currently, 'USB sticks').
Based on the amount to be paid we can have different categorization of mobile payments. Generally we have:

- **Micropayments:** These are the lowest values, typically under $2. Micropayments are expected to boost mobile commerce as well as pay-per-view/click charging schemas.
- **Minipayments:** These are payments between $2 and $20. This targets the purchase of everyday’s small things.
- **Macropayments:** These payments are typically over $20.

Currently, there are several efforts at the international level to accelerate and solidly support emerging mobile payment solutions. Most of the heavyweight companies that deal with hardware or software products for the mobile market and companies such as the mobile network operators (MNO) and financial service providers try via international for a and consortia to define the guidelines to which such a system should comply. The aim is to produce an approach that is widely acceptable and that would reach a global audience and not address just a specific customer base or isolated scenario.

In 2008, relevant mobile access devices fall into the following categories:

- mobile telephones;
- handheld computing devices. These are numerous and diverse, and include personal digital assistants (PDAs) of various kinds, games machines, music-players like the iPod, and 'converged' / multi-function devices such as the Apple iPhone;
- wearable computing devices, such as watches, finger-rings, key-rings, glasses, necklaces, bracelets, anklets and body-piercings;

- processing capabilities housed in other, generally much smaller packages (or 'form factors'), such as credit-cards and RFID tags. Subcutaneous or embedded chips are emergent, and may need to be treated as 'wearable' or as a separate category.

Mobile payments using such devices over such networks may be made in a variety of circumstances (Pousttchi 2003)[115], including:

- MCommerce itself (e.g. the purchase of content, such as location-specific data and audio and video streams);
- the purchase of goods and services in conventional eCommerce in both Business-to-Consumer (B2C) and Business-to-Business (B2B) patterns;
- the purchase of goods and services at conventional points of sale; and
- consumer-to-consumer (C2C) transactions involving transfers of value between individuals.

A considerable technical literature exists, but it is characterised by enthusiasm and narrow focus. Typical of the approach adopted is Herzberg (2003)[22], which focusses on the links and flows between providers, and makes unjustified assumptions about the links and flows between users' devices and providers. Many of the infrastructural features assumed in this literature have not been deployed, or have been deployed but not adopted. In addition, industry coalitions have published technical specifications, such as MPF (2006)[116]. But these lack clear requirements statements against which specific designs and implementations can be assessed. In a survey of paper published in the IS literature between January 2000 and September 2004, Scornavacca et al. (2005)[117] found only 4 of 253 articles that addressed security. By the end of 2007, the specialist M-Business literature index at Scornavacca (2007)[118] contained over 1,100 references, of which 30 had 'security' in the title, 33 had 'payment' in the title, but only one had both (Linck et al. 2006)[119]. Dahlberg et al. (2007)[120] identified three that "discussed technologies in terms of m-payment security", three that "proposed new tools or mechanisms to improve security", and a further four papers of an empirical nature that dealt with security topics. Lee et al. (2004)[121] includes several chapters on the security of mobile transactions. A limited amount of attention has also been paid to it in adjacent literatures, e.g. Choi et al. (2006)[122].

Many authors have considered mobile payments from a technical perspective, but far less attention has been paid to practical application, security aspects, and acceptability by the users of mobile devices. See, however, Rawson (2002)[123] which considered legal aspects of mobile transactions, Pousttchi (2003)[115] and Kreyer et al. (2003)[124] which discussed security as one among many factors in the adoption of mobile commerce, and Zmijewska (2005)[125]. Based on an empirical study, van der Heijden H. (2002)[126] found that "security was emphasized, both for merchants and for consumers, but it was usually framed in a factor that can best be described as 'perceived risk'". Misra & Wickramasinghe (2004)[127] proposed a 'trust model' for mobile commerce generally.

An attempt was made during the late 1990s to impose stronger safeguards. The Secure Electronic Transactions (SET) initiative involved three-way authentication, but foundered in the marketplace (see for example Clarke 1996b)[128]. Since 2000, another attempt is being made, in the form of 3-D Secure, a Visa initiative branded as 'Verified by Visa', and cross-licensed to MasterCard as SecureCode' and to JCB as J/Secure (Visa 2008)[129]. It requires some kind of authentication of the payer's claim to be the cardholder; but it does not specify what form authentication should take, and adoption has been slow.

Table 2.2: Threats and Vulnerabilities Associated with the Access Device
(Roger Clarke 2008[130])

Situation	Threats	Vulnerabilities
The Device as a Whole, incl.: • Hardware, Systems • Software Application Software	Anti-User Design Features Malfunction Attackers Installation of Malware, incl.: • Spyware • Bots • Cracking Tools (e.g. Backdoors, Rootkits) Unauthorised Actions	Lack of User Understanding Bugs (e.g. Buffer Overflows) Insecure Features Insecure Parameter Settings Insecure User Accounts Lack of Product Audit Auto-Download Auto-Execution Remote Invocation Lack of Supplier Warranties and Indemnities Blanket Release of Supplier from Liabilities
Systems Software Specifically	Unauthorised Transactions	Lack of a 'Sandbox' for Applications
Application Software	Unauthorised Transactions	Auto-Storage of Cookies on Server Request Auto-Disclosure of Cookies

Table 2.3: Threats and Vulnerabilities Associated with Transactions

Situation	Threats	Vulnerabilities
Physical Surroundings	Unauthorized Use: • of the Device, incl. Abuse of Privilege • of Authorized Processes Unauthorized Observation,	Lack of Authentication of Local User Lack of Physical Security Safeguards Lack of Logical Security Safeguards

	esp. of Authenticators Coercion Physical Violence Theft	
Manual Processes	Inappropriate User Behaviour, incl.: • accidental (through ignorance) • accidental (through lack of concentration) encouraged or enveigled	Lack of User Understanding Ambient Noise Competition for Attention Susceptibility to Masquerade Susceptibility to Social Engineering (incl. Phishing)
Software Processes	Inappropriate Transaction Partner	Lack of User Understanding Lack of Authentication of Value Being Transferred Lack of Authentication of Partner Identity
	Inappropriate Transaction	Lack of User Understanding Initiation by an Unauthorized User Auto-Initiation Unauthorised Amendment to a Transaction Replay of a Captured Transaction
	Capture of Authenticators (Password, PIN, secret key, private key)	Lack of User Understanding Masquerading Transaction Partner Man-in-the-Middle Attack Resident Malware Insecure Storage Insecure Transmission of Authenticators
	Message Interception	Lack of User Understanding Insecure Transmission of Message

---

Table 2.4: Threats and Vulnerabilities Associated with Other Interactions

Situation	**Threats**	**Vulnerabilities**
Software Download	Anti-User Design Features Malfunction Attackers	Lack of User Understanding Openness to Download driven by a Remote Device
Intrusions	Cracking/'Hacking'	Lack of User Understanding Lack of Authentication of Remote Users Software Errors

		Software Features Malware
Infiltration Vectors	Pre-Installed Software User-Installed Software Viruses Worms	Lack of User Understanding Lack of Authentication of: • Pre-Installed Software Newly-Loaded Software
Infiltration Payloads	Trojans, esp. bot software Spyware, esp.: • software monitors • content monitors • adware • keystroke loggers private key harvesters	Lack of User Understanding Lack of Authentication of: • Pre-Installed Software • Newly-Loaded Software Lack of Checks for Malware Signatures and Malware-Related Behaviour

Table 2.5: Threats and Vulnerabilities Associated with Mobile Infrastructure

Situation	**Threats**	**Vulnerabilities**
Transacting Device	Rogue Device	Lack of Authentication of Transacting Devices
Manual Business Processes	Inappropriate Performance	Lack of Training Laziness Susceptibility to Masquerade Susceptibility to Social Engineering
Data Storage	Second Party: • Inappropriate Access / Abuse of Privilege • Inappropriate Use • Inappropriate Disclosure Third Party: • Inappropriate Access / Abuse of Privilege • Inappropriate Use Inappropriate Disclosure	Lack of Physical Security Safeguards Lack of Access Control Safeguards
Physical Surroundings	Inappropriate Access	Lack of Physical Controls
Computing Facilities	Second Party Third Party	Lack of Access Controls Lack of Organisational Controls Lack of Process Controls
Network Facilities	Second Party: • Inappropriate Access / Abuse of Privilege	Lack of Understanding Messages Sent in Clear Text

	• Inappropriate Use • Inappropriate Disclosure • Inappropriate Amendment • Inappropriate Replay Third Party (Message Interception): • Inappropriate Access / Abuse of Privilege • Inappropriate Use • Inappropriate Disclosure • Amendment Replay	
Supporting Infrastructure	Electrical Air-Conditioning Fire Protection	Malfunction Disabling Attack

2. 9. Conclusion

An overview of past, present, and future mobile banking technologies is presented. This includes review on mobile communication technology, information exchange technology, location identification technology, and security considerations. The chapter also contains an overview mobile communication devices. Technological aspects of various mobile payment technologies are also discussed with their advantages and limitations. Literature review on the various research issues like Online banking, Significance of mobile business activity in financial sector with special emphasis in banking sector, and Security issues on mobile banking transactions are included. Finally a review on mobile payment including various threats and vulnerabilities associated with such financial transactions are presented. The review of literature on mobile banking process and security aspects identifies a gap on advances in technology and actual penetration of such facilities to common mans usage. By developing better, innovative, simple, customer friendly, and more reliable online financial transaction/payment model, banks and other financial organizations can serve the customer needs in better way.

Chapter III

Research Objectives and Methodology

3.1. Introduction

The convergence of the Internet and mobile networks has created new opportunities and applications. Considering mobile business only as an extension of the traditional internet can lead to missing out on unique and differentiable qualities for new value-added opportunities. Mobile banking is considered as potentially one of the most value-added and important mobile services available. The technological changes in mobile networks, mobile devices, and the innovative attributes of mobile internet, advances the theoretical framework of innovation in services allowed to develop a customer centric analysis of m-banking value proposition. The critical factors in the diffusion/penetration of m-Banking, reasons for failure, and further prospects of success depends on various factors and are different for different countries.

In India, the growth of mobile phone subscriber base is increasing in an exponential manner. It is predicted that all inhabited areas (and hence the entire population) of India would be covered by mobile networks by the end of 2011, despite only 65-70per cent coverage today. The number of total mobile subscribers is expected to increase to over 600 million by year-end of 2012. This will support the usage of mobile devices for various kinds of online business and also financial transactions. In this scenario, the Indian banks have to be equipped to start online banking channel as new distribution channel. But, presently, the acceptance of mobile banking services by the Indian customers is not encouraging. It is necessary to find the reason for slow penetration of this value added service in the country. Hence it is planned to study the technological aspects, business model, Indian banks perspective of adopting new innovative distribution channel and the customer’s perspective of accepting this new distribution channel.

3.2 Problem Definition :

Security concerns are the single biggest factor inhibiting consumer acceptance of mobile banking. These concerns are as much a matter of consumer perception as they are of reality. The volume of attacks on mobile banking systems is negligible in the still-nascent and fragmented market that exists today, but will rise as adoption builds, and in particular, as operating system consolidation and platform standardization increases. With a well-designed security program in place, mobile has inherent safety advantages that make it one of the most protected channels for remote banking.

It can be used to improve overall (cross-channel) security via the inherent speed-and-notification advantages of always-on, always -present mobile access. For now, build on the diversity of platforms to maintain confidence that malware isn’t likely to infect consumer devices, but be aware that emergence of standard platforms will erase today’s advantage in the future.

When a consumer identifies a transaction as an unauthorized electronic fund transfer, there is only nominal liability under Regulation of the country. Unlike the closed ATM and credit and debit card networks, the use of wireless technology creates additional risk that information (not limited to financial transaction information) will be stolen, triggering concerns under the privacy provisions of the IT Act. Without the use of highly secure encryption technology to prevent third party data intrusion and losses, the ubiquitous tools of Mobile Finance open the door to enormous potential for monetary as well as reputational risk.

One of the most difficult problems facing banks is the issue of customer authentication. While in many ways a mobile handset is inherently more secure than a desktop computer (for instance, the handset is assigned a distinct telephone number and is owned by a customer with a regular billing or service arrangement with a particular mobile services carrier), the mobility of the device and the nature of wireless communications create additional authentication and security issues for financial institutions and their customers[131].

Will the traditional account number, PIN and test questions suffice for authentication? Will a Financial Institution treat a request to change phone numbers as a "Red Flag"? As is the case with all electronic transactions (wire transfers, ACH and internet banking, for instance), money laundering is also a significant concern in Mobile Banking. The Financial Institution must integrate Mobile Banking into its BSA, AML and OFAC compliance programs. Given that each mobile handset to an extent represents its own teller window, the prospects for financial mischief on a broad scale by techno-savvy bad-guys is very real. Obviously, security issues need to be resolved across the board before one can safely provide these services to even one customer; hence, there are up-front costs that can be intimidating, particularly for smaller financial institutions. Moreover, some regulatory requirements with respect to customer security can exacerbate these costs, making Mobile Banking a costly option for some institutions.

The main goal of this project work are to study and analyze the various security mechanisms/models used in online mobile financial transactions and to improve the security levels by proposing new, innovative security model and protocol which enhances the usage of mobile banking and mobile payment by its simplicity & user friendliness. This Project explores the current technological and security aspects in mobile banking systems. A number of systems like GSM and CDMA offering mobile banking services and highlight their technologies, services and security implementations. The insight of this work is to construct a secure framework for delivery of SMS/WAP banking for authenticated financial transactions. In this project work the focus is on how to achieve security of banking information used in SMS/WAP banking transactions for micro and macro payments.

The other research questions used to find answer in this work are :

1. What are the enabling technologies for mobile banking using a cell phone?
2. What are the security concerns on the enabling technologies used?
3. What security measures are currently deployed with these technologies?
4. What is the appropriate model applicable for secured mobile business financial transactions ?

3.3. Objectives of Present Study

The objectives of this study is to analyze the significance of mobile business activity in terms of their usability, opportunities, and challenges in financial sector with special emphasis on banking activities, to identify the gap between mobile communication technology innovations, their penetration in banking industry as a new distribution channel and the customer acceptance of this new distribution channel, to study present m-business models and their limitations, to propose new business model in order to accelerate the financial transaction process and to provide Value added Services to the customers, and to provide suitable security mechanism to strengthen the mobile business framework in the country.

This also include :

(1) to elicit bankers perspectives to introduce mobile banking as new distribution channel and evaluation of banks strategy to provide and to maintain this new channel.

(2) To examine the customers perspective on mobile banking adoption and its effect on intention and behavior on usage of mobile banking services.

(3) To study various security issues associated with GPRS?WAP networks for mobile banking.

(4) To propose the improved security for mobile banking by studying the suitability of bio-metric identification technique for exact authentication of the customer and hence to avoid fraud in financial transactions.

(5) To study various mobile banking business models, their suitability to Indian scenario and to propose a suitable business model for mobile business through mobile payment to take care of security and authentication problems.

3.4 Scope of the Study

The scope of the solution include all type of micro and macro financial transactions using banking account of the customer for online payments. The model involves authentication of customer identification using bio-metric identification techniques both in SMS banking and WAP banking online payments. Wireless technologies, mobile devices, telecommunications networks and computer systems are the basic infrastructure for supporting anywhere, anytime customer service strategies such as mobile shopping, banking and payments. The interconnectivity and interoperability of networks, systems, and applications have expanded so rapidly and dramatically that the need to implement security measures to protect customers and their data has never been more pressing and challenging.

The scope of the proposal is to explore the mobile business financial services in B-2-C sector. As for the success factors, this study mainly concentrates on business-related success factors for financial institutions and success factors from the customers point-of-view. The findings of the study will throw light on the customer's attitude and behavior on using mobile banking facility and the factors which help to enhance the usage. It may also help in new mobile business model creation based on better security systems adaption, policy-making and to invoke further research.

The focus of the present study is to explore the banker's perspectives to introduce mobile banking as new distribution channel and Customer's perspectives on mobile banking adoption. Hence, exploratory research design is identified as appropriate for the study. The chapter contains an elaborate discussion on responsibility of banks while deploying online banking as new distribution channel through our new "modified customer equity approach model".

In order to explain the customer behavior of adopting mobile banking channel, we have proposed a new model called "Technology Acceptance based on Theory of Customer Stimulation by Education and Training for usage (TCSET). The new model is based on four constructs – perceived usefulness, perceived assurance, perceived ease of use, and perceived cost. These constructs stimulate the customers intention and behavior control to use mobile banking services. The various issues under, customer behavior and intention to use mobile banking transactions, like attitude, trust, convenience, perception, loyalty, privacy, security and comfort issues are discussed based on the developed model.

3.5. Conceptual Study on Banker's Perspectives on Mobile Banking

Providing financial transactions through mobile devices is a new distribution channel for financial institutions. Using this new distribution channel, they can add further value to their financial services. One of the industries which seem to be more affected after inventing internet and mobile communication technology is retail banking. It holds all the opportunities and threats connected with the mobile devices and the mobile communication technology. Many retail banks have a dense branch network, close relationships with their customers, and are mostly local businesses operating in one country or part of a country or selected locations of the country only. However, their core services are perfectly digitizable and the new technology therefore has a potential for transferring all their banking business to mobile banking. This availability of new distribution channel is interesting for banks for many reasons due to possibility of improving operation effectiveness and service differentiation :

1. The new electronic distribution channel can offer the customers better service output in the form of a broader and deeper assortment, less waiting time, and higher market decentralization. This may attract new customers (Mols et al., 1999)[131], increase the revenue of the innovative firms and consequently lead to higher profits over a long period of time.
2. The new electronic distribution channels are more cost effective than telephone and branch based networks, and lower cost may lead to lower prices for the consumers. In such cases, seemingly loyal customers may change to the new distribution channels, and the firms that have invested in the wrong channels may end up with channels that turn out to be useless, i.e., investments which may be difficult to recover.
3. The new electronic distribution channels may change the way in which financial institutions interact with their customers and may facilitate direct marketing, relationship marketing and mass customization and thus increase customer loyalty.
4. The number of customers demanding mobile banking channel is likely to increase in the future. With the increase in literacy and the availability of mobile phones at cheaper rate and fall in the cost of mobile communication charges, there has been a considerable growth in the segment of customers preferring mobile banking. This will change the optimal distribution channel structure for the most retail banks.

Since the distribution channels changes very slowly, the need to act quickly has less obvious than in areas such as new product development, pricing and advertising. Before the widespread acceptance of internet banking and mobile banking, retail banks gained competitive advantage by adding new branches. These branches are expensive and no bank could afford to establish branches in every town. This resulted in differences in coverage and usually those banks which are the first to build a large network in an area gained a strong and lasting lead. Thus a right investment in distribution channels have traditionally been a long term protection against competition, and few researchers have been concerned with proposing strategic design principles focusing on feedback mechanisms to continuously monitor the design of distribution channels.

3. 5.1. Responsibility of Banks

Deploying online banking as a component of a customer equity-building strategy of present Indian banks may be the best way to succeed. The customer equity approach model (Fig 3.1) proposed in this work is based on a long-term strategy of acquiring, retaining and selling additional services to the desired customer and online banking capabilities could help banks to improve their efforts in acquisition and retention of the customers. An integrated online and offline channels can be effectively used by the banks to acquire new customers. Websites that provide helpful information could attract prospective customers to investigate further products and services offered by the bank. These prospects can then use their preferred channels (online, telephone or a branch) to open a new account or apply for a loan. Online capabilities could be extremely helpful in retaining customers. By facilitating interaction and two-way communications, banks can learn about problems and opportunities before it becomes too late or costly to recover. Retention of individual customers can be enhanced as well as the ability to identify emerging service trends that may affect many customers. The last phase of a customer equity approach calls for increasing sales of additional products and services to existing customers. Additional sales contribute to increased profitability as well as to cementing the relationship with individual customers. The opportunities to use online capabilities to increase sales are enormous; most banks have not even scratched the surface of what is possible. Most sales efforts to date have been product-centric with little attention to the needs of individual customers. The online world allows banks to move proactively into customer-based marketing efforts. By developing meaningful databases, monitoring consumer needs and behavior, and experimenting with different tactics, new revenue streams are likely to materialize.

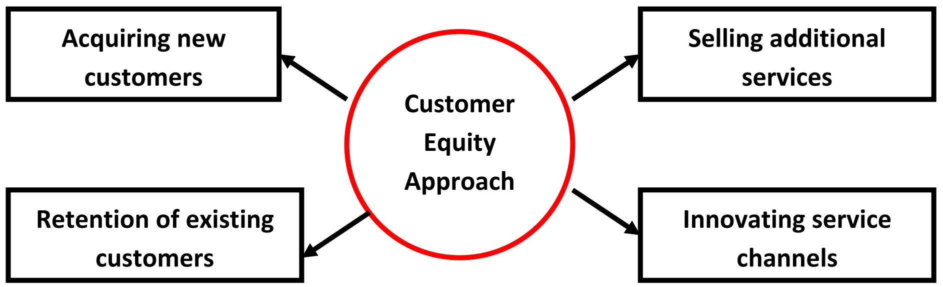

Acquiring new customers
Selling additional services
Customer Equity Approach
Retention of existing customers
Innovating service channels

Fig 3.1 : Modified Customer Equity Approach Model.

In sum, a new goal of using online capabilities to acquire, retain and sell additional services to desirable customers is very feasible. To be able to get there, however, banks still face the challenge of convincing more customers to bank online. Thus, both for cost reduction and customer equity goals, banks need to find ways to accelerate the rate of consumer adoption of online banking. Only by pushing forward banks can hope to derive the benefit from the opportunities outlined above. Yet, for most banks, the efforts to date have not been very successful.

3.6. Conceptual Study on Customers Perspective on Mobile Banking

Generally, studies of adoption of information technology takes one of three possible approaches, *a diffusion approach, an adoption approach or a domestication approach.* Diffusion researchers typically describe the aggregate acceptance process as a function of time that may be used to categorize adopters of different kinds (Mahajan et al., 1990)[132]. Others like, Rogers (1995)[133] describe the *diffusion* process as consisting of four elements: an innovation or new technology, a social system, the communication channels of the social system and time. *Adoption* researchers, on the other hand, typically describe and explain the acceptance decision of individual users applying different social theories of decision-making. Three models, collectively called the Technology Acceptance Theories (TAT), stand out as the most widely applied explanation within the adoption approach. Research literature states that information about technological innovations can travel through a variety of communication sources and modes to members of a social system (Roger, 1995)[133] have found that communication factors are also significant predictors of customer adoption of electronic banking innovations. New product innovators in technology based products are likely to be drawn from heavy users of other products within the product category. Adopters who adopt earlier than others are likely to gain more from the use of the product and hence have a greater usage propensity. Additionally, it is argued that adoption of complex products depends on the adopter’s ability to develop new knowledge and new patterns of experience. This ability can be enhanced by the knowledge gained from related products or the proper education on the new product and training on how to use it. In India, the educational and economical level of the people is not so advanced like other advanced countries where the above acceptance theory is used to study the customers' behavior on new technology based products acceptance. Here, a new product usage can be enhanced by giving proper education on the product and training to use it. Accordingly, in this study, the Technological Acceptance Model is modified by considering local communication factors.

3.6.1. Modified Technology Acceptance Theory

In addition to three models proposed under Technological acceptance theories (TAT), this study proposes a new model which is a modification of Technology Acceptance Model and named as **Technology Acceptance Based on Theory of Customer Stimulation by Education and Training for Usage (TCSET).** As in TRA, it includes behavioral attitudes, subjective norms, intention to use and actual use based on user training. However, this theory interprets *behavioral control based on knowledge and training.* Perceived behavioral control covers both the intention to use and the actual usage. Actual usage is in turn a weighted function of intention to use and perceived behavioral control based on knowledge of that technology and training on usage of such technology.

According to this model, any innovation in Technology and its application in service sector gets popularity if that innovation reaches the end user through education and training. Customer Education provides knowledge about that innovation and its relative advantages over conventional service model to the customers. The training provided by the service provider allows customer familiarize him/her to use that innovation. **Customer education** leads to knowledge about innovation, which in turn influence the perceived usefulness and perceived assurance of the innovation. In case of online mobile banking, Ubiquitous service, Enhanced Productivity due to adapting new innovation, Time saving, Opportunity for better service, Status in the Society, Challenging environment, may be <u>perceived usefulness</u> for the customers and Security of Information. Accuracy of transaction and Reliability of service are <u>perceived assurance</u> for the customers. **Customer Training** influences the <u>perceived ease of use</u> of that innovation compared to traditional model. This also influences the customer <u>perception on cost</u> of the new innovation.

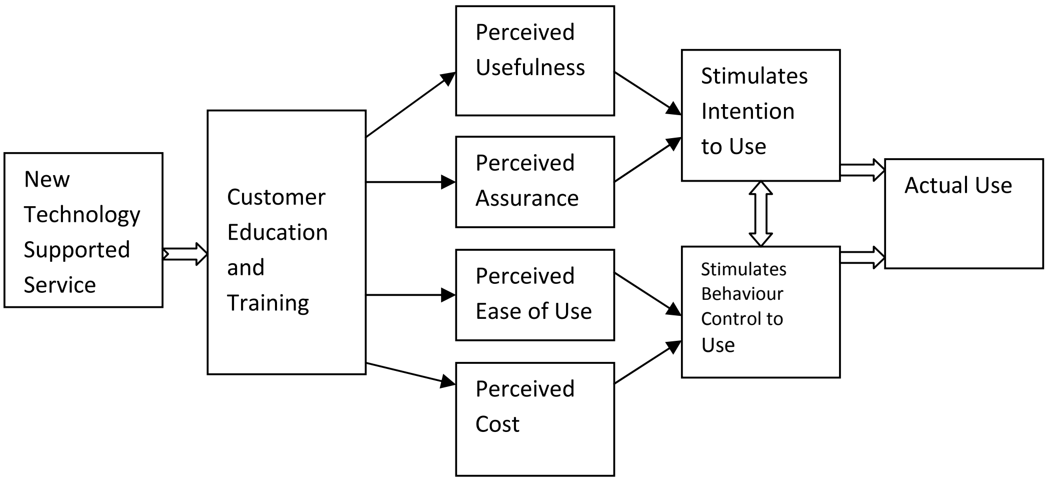

New Technology Supported Service
Customer Education and Training
Perceived Usefulness
Perceived Assurance
Perceived Ease of Use
Perceived Cost
Stimulates Intention to Use
Stimulates Behaviour Control to Use
Actual Use

Fig. 3.2 : Technology Acceptance Model : Theory of Customer Stimulation by Education and Training for Usage (TCSET)

(Our research Model)

Perceived Usefulness :

1. Ubiquitous service
2. Enhanced Productivity
3. Time saving
4. Opportunity for better service
5. Status in the Society
6. Challenging

Convenience
Better service
Speed of service

Perceived Ease of Use :

1. Easy Operation of the device
2. Easy and simple method of obtaining service
3. Bundled services
4. Availability of services & Network
5. Ease of switching between new and old models
6. Ease of making corrections
7. Ease of Registration to the bank

Attitude
Loyalty
Perception

Perceived Cost :

1. Low device cost
2. Low service cost
3. Avoiding inter-mediatories
4. Low transaction cost
5. Low cost registration for availing service
6. Zero hidden cost

Loyalty
Attraction

Perceived Assurance :

1. Security of customer Information
2. Accuracy of transaction information
3. Reliability of service

Risk free
Trust

In case of online mobile banking services, the perceived ease of use include : easy operation of the device, easy and simple method of obtaining service, bundled services, availability of services and network, ease of switching between new and old models, ease of making corrections, and ease of registration to the bank. The perceived cost involves the knowledge on cost of device, service cost, avoiding inter-mediatories, transaction cost, low cost registration for availing service, hidden cost etc.

The perceived usefulness of the innovation and perceived assurance stimulates the intention of customers to adapt new innovation and the perceived ease of use and the perceived cost of innovation stimulates the behavioral control of customer to use the new innovation. This model is more meaningful and applicable in developing and underdeveloped countries because of the low educational background and shy nature of rural people. To penetrate such innovative new service models effectively and efficiently, service providers should involve in customer education and training to stimulate the behavioral control and intention of the customer to adapt new service in their daily life.

TCSET adopts the following causal chain :

Innovation > Education and Training > Stimulation > Intention > Behavior > Actual usage

Stimulation = f(education and training)

Intention = f(usefulness and assurance)

Behavior = f(ease and cheap)

The three key stimulations that specially account for new innovation usage. The first of these beliefs is perceived usefulness, defined as ‘the degree to which a person believes that using a particular system would enhance his/her job performance’. The second is perceived ease of use, defined as 'the degree to which a person believes that using a particular system would be free of effort’. The third is perceived cost, defined as ‘the degree to which a person believes that using that system is cost effective and reduces his expenditure substantially’.

The most basic proposition of the TCSET is Customer Stimulation (S_C) and is a function of Stimulative Behavior (S_B) and Stimulative Intention(S_I). In previous models the behavior is postulated as a function of the individual’s attitude toward the act and the social norms. Whether the attitude toward the act or the social norms exerts the greater influence on the behavioral depends on the individual and the decision object (Ajzen and Fishbein, 1980)[134].

However, in our model we predict that individuals stimulative behavior is a function of ease of availing and performing service action (ease of use) and the comparative cost advantage (cheap). Therefore, it can be written as:

$S_B = f_1$ (perceived ease of use) + f_2 (perceived cheap of service) --------- (1)

The parameters f_1 and f_2 each reflect the strength of the relative impact of the ease of use and cost advantage of the service on the stimulative behavioral decision. The stimulative intention toward the adoption of the service is determined by the individual's beliefs on perceived usefulness (P_u).

That is:

$S_I = f_3$ (perceived usefulness) + f_4 (perceived assurance) ------------ (2)

Based on above, the customer stimulation S_C is defined as the algebraic sum of individuals perceived usefulness, perceived assurance, perceived ease and perceived cost effectiveness.

$S_C = f(S_B + S_I)$ ------------ (3)

i.e. $S_C = f_1(P_E) + f_2(P_C) + f_3(P_U) + f_4(P_a)$ ------------ (4)

where P_E, P_C and P_U P_a are perceived ease, perceived cost, perceived usefulness and perceived assurance.

3.6.2. TCSET Model applied to Online Mobile Banking

Online mobile banking services is a new distribution channel for financial services for the banks. Adapting such distribution channels for basic services like, account checking, finding last few transactions, Cheque book request etc. will enhance banks obligation to provide ubiquitous service. Educating the old customers and the new customers by providing Training on how to use and get benefit by using these services anywhere any time without fear. When the customer understands the easiness of operation and advantages of financial transaction using online mobile device in terms of cost benefit and other usefulness, he/she will tempted to use such distribution channel for future transactions by making use of his mobile set. Hence providing education and training to present customers, bank can teach the customers about perceived usefulness, perceived ease of operation of mobile device to make transactions and perceived cost-benefit by using such transactions frequently. This kind of training provided to the customers will certainly stimulate the intension to use such facility frequently and it also stimulates the behavior control to use such facility. Such stimulation of behaviour and intension due to perceived ease, perceived cost and perceived usefulness of mobile banking channel for ubiquitous financial transaction.

Thus the customers who have mobile phone will be educated towards the advantages of this channel, get trained to reduce hesitation of usage of mobile banking channel and hence considerable improvement is possible due to changes in behaviour and intension of usage. The education and training camps conducted by the banks not only stimulate the existing customers of the banks but it will attract new customers to the bank due to percolating effect.

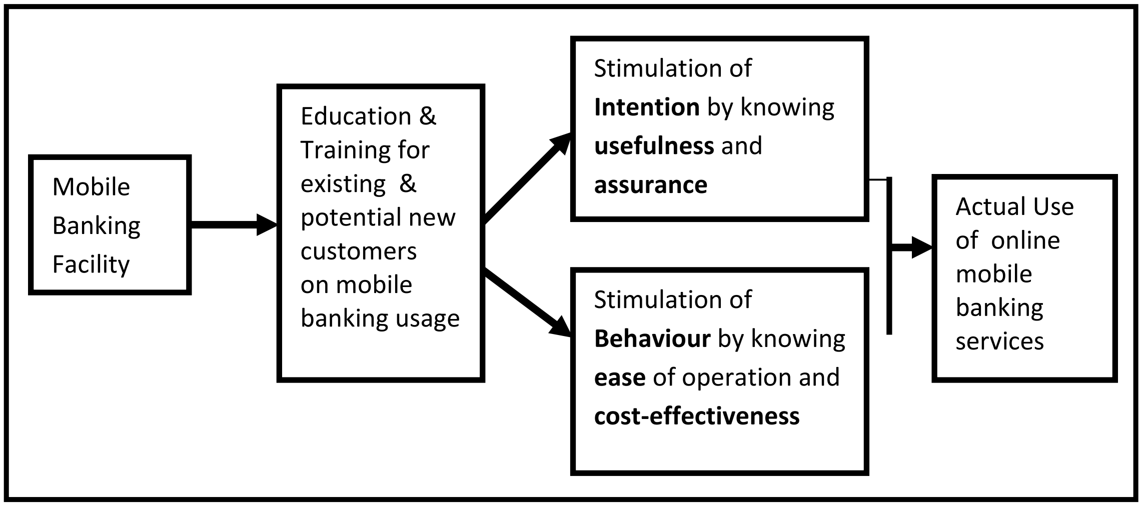

Mobile Banking Facility
Education & Training for existing & potential new customers on mobile banking usage
Stimulation of **Intention** by knowing **usefulness** and **assurance**
Stimulation of **Behaviour** by knowing **ease** of operation and **cost-effectiveness**
Actual Use of online mobile banking services

Figure 3.3 : TCSET Model applied to Online Mobile Banking

Issues Effecting the Intention and Behavior :

(a) Attitude

Attitude is defined as an individual's positive or negative feelings (evaluative affect) about performing a target behavior (Fishbein and Ajzen, 1975)[135]. It is related to behavioral intention because people form intentions to perform behaviors toward which they have positive affect. Taylor and Todd (1995)[136] suggest that the different dimensions of attitudinal belief toward an innovation can be measured using the five perceived attributes like relative advantage, compatibility, complexity, and trialability of an innovation. These attribute, originally proposed in the diffusion of innovations theory (Rogers, 1995)[133], are applied in this framework. Perceived relative advantage of an innovation like online banking is positively related to its rate of adoption. Online banking services allow customers to access their banking accounts from any location, at any time of the day, it provides tremendous advantage and convenience to users. It also gives customers greater control over managing their finances, as they are able to check their accounts, transact funds easily. In view of the advantages that online banking services offer, it would thus be expected that individuals who perceive online banking as advantageous would also be likely to adopt the service.

Online banking has been viewed as a delivery channel that is compatible with the profile of the modern day banking customer, who is likely to be computer-literate and familiar with the Internet.

Therefore, it is expected that the more the individual uses online devices, and the more he or she perceives them as compatible with his or her lifestyle, the more likely that the individual will adopt Online banking. Online banking can be seen as an expeditious tool that allows customers to better manage their multiple accounts. As there are more financial products and services, it is expected that individuals who may have many financial accounts and who subscribe to many banking services will be more inclined to adopt online banking. As the online banking devices are very user friendly, it is likely that potential customers may feel that online banking services are less complex to use, and hence would be likely to use such services. Thus the lower the perceived complexity of using online banking, the more likely that it will be adopted. If customers are given the opportunity to try the innovation by means of education and training, certain fears of the unknown may be minimized. This is especially true when customers find that mistakes could be rectified, thus providing a predictable situation. Similarly, it is expected that only individuals who perceive using Internet banking as a low risk undertaking would be inclined to adopt it.

(b) Trust

Building customer trust in online mobile banking is a continuous process, which extends from initial trust formation to continuous trust development. The reliability and security needed to cultivate online trust are equally important for online banking transactions through internet or mobile technology. Extra emphasis should be placed on developing banks reputation because of the novel nature of mobile banking. A good reputation suggests certainty and less risk in conducting business, and thus helps foster customer trust. The factors like high quality information, attractive rewards, easy connectivity, multiple level passwords for high level security are plays important roll in building initial trust. The factors like quick transactions, maintaining banks' integrity, strengthen security controls, and providing additional financial supports provides continuous trust developments and maintenance.

(c) Convenience

One of the greatest advantage of online banking services is convenience. Unlike retail banking, customers need not travel to their physical bank branches, need not weight in a long queue, need not move from window to window for availing the banking services and need not vary about banking timings. Through online mobile devices, they can login to their banking account from anywhere, at any time for financial transactions and utility bill payments. Along with improved convenience, online mobile banking reduces cost of financial transactions. Presently most of the Indian customers use either internet based or mobile phone based online banking services. Such transactions cost less than Rs. 1 compared to cost incurred by retail conventional banking. By using mobile devices such as mobile phones, customers can carryout financial transactions at anywhere and at any time. Such ubiquitous service certainly boost the usability of online banking services in India. Educating and training the customers to use online banking services through their mobile phone is one of the immediate requirement for all conventional banks to convert their customers to adopt online banking services. Convenience, market forces, and speed are just some of the many reasons that over half of all banking transactions do not take place in a traditional branch. Consumers want instant access, in many different forms. However, there are opportunities to "modernize" banking transactions even further. One of these is the ability to view through alternative banking delivery mechanisms, images (pictures) of checks and deposits made by customers to a bank.

(d) Perception :

For a number of individuals, usage and attitudes to technologically facilitated services are influenced by perceptions of how reliably and easily the system caters for their needs. As a consequence, for some customers their perception of the advantages offered by the service used is influenced by their perception of the system's operational efficiency and reliability, ease of access and use. System complexity and clutter, crashes, drop outs, malfunctions and their consequential delays, if experienced regularly, can serve to inhibit regular use and provoke negative attitudes to both the service provider and the system generally. Therefore for marketed benefits of mobile banking services to be plausible and credible they must be consistently delivered and maintained by the mechanics of the system. Moreover, for a customer–service provider relationship to be established, nurtured and maintained, the facilitating means of service provision must function in a manner that enables and supports this effectively and reliably. It can be argued that more care needs to be taken to ensure that services and systems are designed more from a user perspective and in a way that enables users to complete their desired transactions straightforwardly, quickly and efficiently, in a way that enhances rather than impedes accessibility, and that fosters positive rather than negative attitudes on the part of the customer. In turn, these positive attitudes will more likely serve to foster the sense of trust and commitment necessary to the customer's sense of relationship with the service provider.

(e) Loyalty :

It has been shown that customer loyalty derives from one's trust in, and commitment to the service provider fostered over time (Sirdeshmukh et al. 2002)[137]. The relationships in which trust and commitment are inherent elements encourage loyalty. It is therefore reasonable to argue that customer loyalty to a service provider in virtual market space will depend, inter alliance, on the trust that a customer has in the service provider and what is offered, as well as the extent to which they believe they can trust and rely on the manner of service delivery or provision. Correspondingly, their loyalty will also be born of, and manifest as, a sense of attachment and commitment to the service provider for reasons both instrumental and emotional. This also suggest that customer trust in, and commitment to, individual banks may be disaffected as a consequence of dissatisfying experiences with their use of online mobile banking services, and by residual negative attitudes to the service provider. In other words, the experience of customers with banking services provided in this way, combined with their residual attitudes to banks, combine to create an attitude that may be antithetic to fostering a sense of relationship with the service provider (Walker et al., 2000)[138].

(f) Privacy, Security and Comfort Issues :

In on-line mobile banking, identity theft is rapidly becoming a serious problem that impacts both customers and service providers. As more and more people are turning towards the internet through mobile device to make their financial transitions, these users and the websites that they are using are becoming inviting targets for identity theft. It is relatively easy to obtain personal information via the web, and by using the internet to make purchases these consumers' personal information is being released for a variety of purposes over the web.

When exploring solutions to the problem of identity theft, one could simply not to pay any bills or purchase anything online. As this is sometimes impossible and not desirable, the only logical solution is to be cautious and protect oneself. Thus, when paying bills or purchasing merchandise over the web, consumers are taking the risk that someone will access their personal information and use it in a fraudulent manner. Consumers can do much to prevent becoming the victims of identity theft. Essentially, consumers can either take the time to develop preventative strategies or take the risk of identity theft. Many consumers are proactive in this area with the aid of the online financial institutions that serve them, while others do not know how to check the security of websites and therefore avoid using the internet at all to do their online mobile banking, which can also have a negative effect on businesses. With the overwhelming fears of identity theft, it is critical for many businesses, especially banks that operate online to develop better ways to ensure the security of their websites. One of the most important steps an online bank needs to do to create better site security is to analyze their current systems. "As transactional systems and online traffic have become more common, lapses in current systems have led to breaches that have been real doozies" (Bielski, 2003, p.53)[139]. Owing to these lapses, several companies have fallen victim to the misuse of several of their sites. Next, online banks need to do is to identify their weakest points in their systems and improve them. “Most security experts agree that outsiders can and do get passwords and data on a fairly regular basis … much of the mayhem could have been avoided with a more organized approach to security or use of newer tools”. When online banks bring in the newest technologies within the shortest amounts of time, there usually is less possibility that hackers could find their way into the systems. By the time many hackers figure out the old system, the new systems will already be in place.

Online banks need to create customer service strategies that make a more secure site through simple personal-based maintenance protocols. Management must understand that all financial information that is networked is vulnerable without innovative security schema to protect it. To be constantly aware of how secure their systems are, they need to continuously analyze their systems. For example, Meta Security Group is one of the many firms that conduct security audits for online banks and other security conscious companies with e-enterprises (Bielski, 2003)[139]. If banks have to use such outsourcing sources, they could forfeit the internal costs of paying to train people to do these kinds of audits as well as providing for third-party audits, a very sound procedure after the recent Enron and Anderson financial audit disasters. It would not only decrease their costs, but it would also improve their systems by having professionals who are trained for some years to analyze systems looking for problems. If online banks or any other business are to incorporate all these matters, there may be having less fear concerning security attacks.

3.7 Requirements to next-generation mobile payment systems

When looking at the advantages and drawbacks of existing payment methods and when learning from the reasons why many payment systems failed, one can derive a set of technical, business, and user requirements:

• Interoperability

Financial networks follow the three domain model in order to implement interoperability. Brand and business rules are defined in a payment scheme. Issuers hold contracts with consumers, maintain consumer accounts and issue e.g. credit cards. Merchant acquirers deliver services tailored to merchants’ needs. The interchange domain ensures interoperability, computes fees and settles funds between issuers and acquirers. Stakeholders are not restricted to a single role, e.g. some banks issue cards and acquire merchants at the same time. Technically, interoperability is achieved by standardized protocols like ISO 8583.

• Wide-spread acceptance

Every introducer of a new payment system encounters the so-called hen-and-egg problem. Consumers are reluctant to use and subscribe for a new payment method, as long as acceptance is limited to a small subset of merchants; merchants hesitate to accept a new scheme as long as the consumer base is small. Leveraging the existing infrastructure (merchant acquirers, issuers) can overcome this problem.

• Ease of use

Consumers and merchants are familiar with use cases like registration, confirming payments with a PIN, transactions (e.g. credit and debit), account statements, etc. Ease of use can be achieved if a mobile payment scheme copies the known payment transaction types, use cases, and business relationships. Moreover, a payment system of international scope is expected to provide foreign currency conversion during the payment flow.

• Disposability

The need of additional devices or software poses a barrier for introducing a new payment system, in particular to consumers. Furthermore, consumers prefer payment systems that provide ubiquitous access. A method bound to e.g. a PC (like some e-cash schemes) limits usage to web payments and is likely to remain in this niche segment.

• Economy

Cost for deploying and maintaining a new payment method as well as subscription and per transaction fees must compete with costs of existing payment schemes. On the other hand, fee distribution among the service providers must cover their efforts and risks.

• Security

Strong payer authentication is the precondition to prevent consumer fraud and to keep the number of disputes low. This is why most schemes that provide a payments guarantee for the payee demand strong consumer authentication. Measures for integrity, non-repudiation, confidentiality, and persistence further reduce the number of disputes and increase consumer trust.

• Anonymity

The consumer prefers anonymous payments, which is in contrast to fraud reduction and strong authentication. Nevertheless, consumer data can be hidden from the merchant while still keeping strong authentication by the issuer. The requirements listed above are considered the most important technical, user, and business requirements.

3.8. GSM AND GPRS Security Architecture

Global System for Mobile Communications (GSM) is the most popular standard for mobile phones in the world. Figure 3.4 shows the basic structure of the GSM architecture; GSM provides SMS and GPRS (General Packet Radio Service) services. The GPRS Core network is an integrated part of the GSM network; it is layered over the underlying GSM network, with added nodes to cater for packet switching. GPRS also uses some of the existing GSM network elements; some of these include existing Base Station Subsystems (BSS), Mobile Switching Centers (MSC), Authentication Centers (AUC), and Home Location Registers (HLR). Some of the added GPRS network elements to the existing GSM network include; GPRS Support Nodes (GSN), GPRS tunneling protocol (GTP), Access points, and the (Packet Data Protocol) PDP Context.

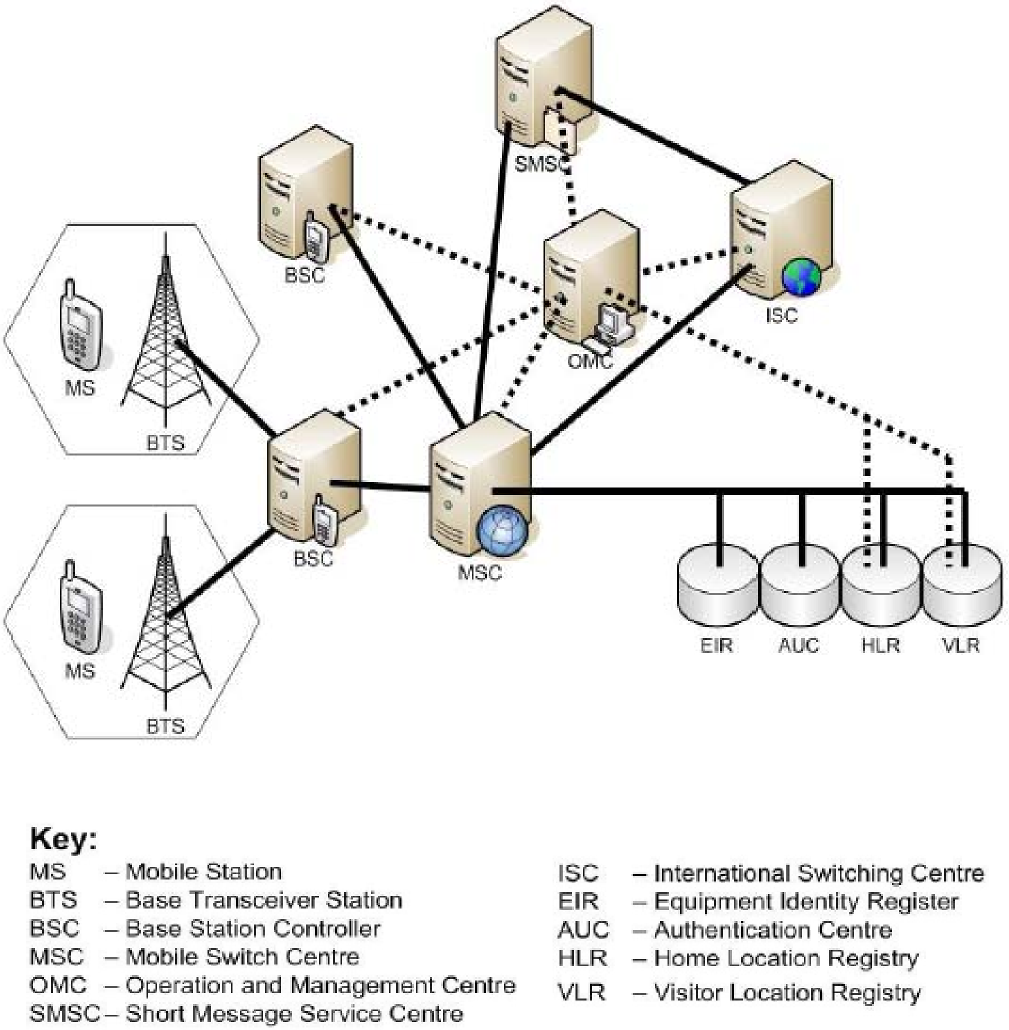

SMSC
BSC
ISC
OMC
MS
BTS
BSC
MSC
EIR
AUC
HLR
VLR
MS
BTS
Key:
MS – Mobile Station
BTS – Base Transceiver Station
BSC – Base Station Controller
MSC – Mobile Switch Centre
OMC – Operation and Management Centre
SMSC – Short Message Service Centre
ISC – International Switching Centre
EIR – Equipment Identity Register
AUC – Authentication Centre
HLR – Home Location Registry
VLR – Visitor Location Registry

Figure 3.4. GSM Architecture

3.8.1 Security mechanisms in the GSM network

The GSM network has some security mechanism to prevent activities like Subscriber Interface Module (SIM) cloning, and stop illegally used handsets. GSM has methods to authenticate and encrypt data exchanged on the network.

1. GSM Authentication Center

The GSM authentication center is used to authenticate each SIM card that attempts to connect to the GSM network. The SIM card authentication takes place when a mobile station initially attempts to connect to the network, i.e. when a terminal is switched on. If authentication fails then no services are offered by the network operator, otherwise the (Serving GPRS Support Node) SGSN and HLR is allowed to manage the services associated with the SIM card.

2. Authentication Procedure

The authentication of the SIM depends on a shared secret key between SIM card and the AUC called Ki. This secret key is embedded into the SIM card during manufacture, and it is also securely replicated into the AUC. When the AUC authenticates a SIM, it generates a random

number known as the RAND. It sends this RAND number to the subscriber. Both the AUC and SIM feed the Ki and RAND values into the A3/A8 (or operator proprietary algorithm (COMP128)) and a number known as Signed RESponse (SRES) is generated by both parties. If the SIM SRES matches the AUC SRES the SIM is successfully authenticated. Both the AUC and SIM can calculate a second secret key called Kc by feeding the Ki and the RAND value into the A5 algorithm. This would be used to encrypt and decrypt the session communications. After the SIM authentication the SGSN or HLR requests the mobile identity, this is done to make sure that the mobile station being used by the user is not black listed. The mobile returns the IMEI (International Mobile Equipment Identity) number; this number is forwarded to the EIR (Equipment Identity Register). The EIR authorizes the subscriber and responds back to the SIM with the status, if the mobile is authorized the SGSN informs the HLR and PDP Context activation begins.

3.8.2 Problems with GSM Network

1. Problems with the A3/A8 authentication algorithm

A3/A8 is the term used to describe the mechanism used to authenticate a handset on a mobile phone network [140]. A3 and A8 are not actually encryption algorithms, but placeholders. In A3/A8 the commonly used algorithm is COMP128 [141]. COMP128 was broken by Wagner and Goldberg in less than a day [142]. This raises concerns of having GPRS as a secure communication mechanism. After cracking COMP128 Wagner and Goldberg went on to prove that it was possible to obtain the Ki value, therefore making it possible to perform SIM cloning. There has been a release of COMP128-2 and COMP128-3 to cater for some of the SIM cloning issues, but the majority of the SIMs still being used use COMP128.

These security threats illustrate some of the security issues which should be rectified if GPRS is to be used as a secure medium for mobile banking.

2. Problems with A5 algorithm

The A5 algorithm is used to prevent casual eavesdropping by encrypting communications between mobile station (handset) and BSS. Kc is the Ki and RAND value fed into the A5 algorithm. This Kc value is the secret key used with the A5 algorithm for encryption between the mobile station and BSS.

There are at least three flavours of the A5 algorithm. These include A5/1 which is commonly used in western countries. The A5/1 is deemed strong encryption [142] but it was reverse engineered some time ago. A5/2 has been cracked by Wagner and Goldberg, the methodology they used required five clock cycles making A5/2 almost useless. Finally A5/0 is a form of A5 that does not encrypt data at all.

All these problems with the A5 encryption algorithms prove that eavesdropping between mobile station and BSS is still possible, making GPRS over the GSM core network very insecure for mobile banking.

3. Attack on the RAND value

When the AUC attempts to authenticate a SIM card, the RAND value sent to the SIM card can be modified by an intruder failing the authentication. This may cause a denial of service attack [142].

3.8.3. Current SMS Banking Services

Currently most of the banks, use the Wireless Internet Gateway (WIG) for mobile banking. They uses the Unstructured Supplementary Services Data (USSD) with SMS approach. Some banks uses a model which requires the user to first send a USSD string with the user's PIN to the banking server. Then the server returns a message to notify the user that the server is ready to accept banking SMS message. This approach is not secure because every user s detail is transmitted in plaintext. The mobile network operator has full access into the banking details sent by the user.

Security Problems with SMS

The initial idea for SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, end-to-end security, nonrepudiation were omitted during the design of GSM architecture [142]. Some of the security problems of using SMS are :

1. Forging Originator s Address

SMS spoofing is an attack that involves a third party sending out SMS messages that appear to be from a legit sender. It is possible to alter the originator s address field in the SMS header to another alpha-numerical string. It hides the original sender s address [139] and the sender can send out hoax messages and performs masquerading attacks.

2. SMS Encryption

The default data format for SMS messages is in plaintext. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. Endto-end encryption is currently not available. The encryption algorithm used is A5 which is proven to be vulnerable [142]. Therefore a more secure algorithm is needed.

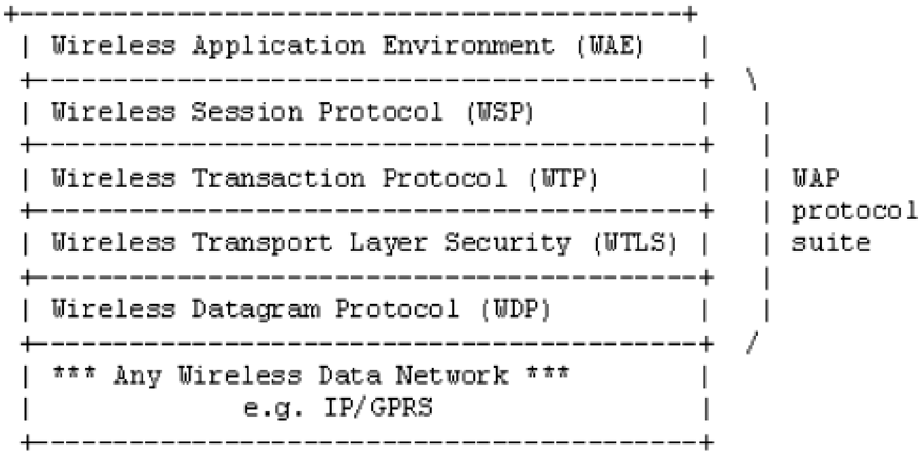
3.8.4. Current GPRS Implementations

1. Present GPRS banking implementations

Presently most of the banks are using the MTN mobile banking gateway. MTN mobile banking allows bank account holders to access WAP sites and perform banking the same way they would carry out internet banking.

2. Wireless Application Protocol (WAP)

WAP is an open international standard for applications that uses wireless communication. Its principal application is to enable access to the internet from a mobile phone or PDA [143]. Mobile phones or terminals can access the internet using WAP browsers; WAP browsers can only access WAP sites. Instead of the traditional HTML, XML or XHTML, WAP sites are written in WML (Wireless Markup Language). The WAP protocol is only persistent from the client to the WAP gateway, the connection from the WAP Gateway to the Bank Server is secured by either SSL or TLS. Figure 3.5 below illustrates this architecture. WAP provides security of communications using the WTLS (WAP Transport Layer Security) protocol and the WIM (WAP Identity Module). WTLS provides a public-key based security mechanism similar to TLS and the WIM stores the secret keys. In order to allow the interoperability of WAP equipment and software with many different technologies WAP uses the WAP protocol suite.



```
+------------------------------------------+
 | Wireless Application Environment (WAE)   |
 +------------------------------------------+  \
 | Wireless Session Protocol (WSP)          |   |
 +------------------------------------------+   |
 | Wireless Transaction Protocol (WTP)      |   | WAP
 +------------------------------------------+   | protocol
 | Wireless Transport Layer Security (WTLS) |   | suite
 +------------------------------------------+   |
 | Wireless Datagram Protocol (WDP)         |   |
 +------------------------------------------+  /
 | *** Any Wireless Data Network ***        |
 |             e.g. IP/GPRS                 |
 +------------------------------------------+
```

Figure 3.5 WAP Protocol Suite Source from [136]

1. Security problems with Current GPRS/WAP Implementations

1. Security issues with present implementations that use WAP

The present mobile banking implementations that are using WAP have proven to be very secure, but there exist some loopholes which could lead to insecure communications. Some of these loopholes include:

☛ There is no end-to-end encryption between client and bank server. There is end-to-end to encryption between the client and the Gateway and between the Gateway and the Bank Server. To resolve this, the bank server could have its own Access Point Name (APN) in any of the GPRS networks. This APN would serve as the WAP Gateway for the bank. Therefore the client would be connected directly to the bank without third parties in the middle of the communication.

☛ Public key cryptosystems key sizes offered by the WTLS standard are not strong enough to meet today s WAP applications security requirements. Considering the low processing power of the handheld devices, the key sizes have been restricted [144].

☛ Anonymous key exchange suites offered by the WTLS handshake are not considered secure. Neither client nor the server is authenticated. Banks should provide functionality to disallow this option of handshaking.

2. Security issues associated with using the plain GPRS network

The GPRS core network is too general; it does not cater for some banking security requirements. Some of these requirements include:

☛ Lack of account holder or bank authentication. The Bank can provide a unique APN to access the Bank server, but without this or some other authentication mechanism anyone can masquerade as the Bank. All these issues raise concerns of fabrication of either bank information or account holder information.

☛ Provision of functions to avoid modification of data and ensure the integrity of data for both the account holder and the Bank.

☛ The methods to cater for confidentiality of data between the mobile station and the bank server have proven to be weak, and the network operator can view account holder s information. This raises security issues for both the bank and account holder.

☛ The bank cannot prove that the account holder performed a specific action and the account holder cannot prove that the bank performed a specific action.

☛ GPRS provides session handling facilities, but does not handle Bank specific sessions; this may cause inconsistencies on the bank s side raising security issues.

A bank will mostly require more security functionality than an ordinary browser is able to provide. This extra security functionality included strong cryptography. A dedicated standalone client/server application is therefore an alternative way to realize communication between the user/customer and the bank. The same protocol as used by the Web browser/server can be used here to provide security. However, the bank must provide the user/customer with the necessary software, as the electronic banking system does not rely on the browser that is already installed on the user's mobile device. To avoid the problem of distribution and installation of extra software on the user's mobile device, banks often deploy an intermediate solution. An ordinary browser is used at the client side, but to increase the functionality, a Java applet is downloaded from the bank's website. This applet is a relatively small piece of software code that runs within the user's browser, and that will provide extra security functionality. A big advantage of this approach is that the applet technology allows the bank to easily maintain and update the client software. Clients will automatically download and use new versions of the software. Banks do not need to distribute new software in an old-fashioned way. Note that in the scope of this paper we intend to use the term user when we want to refer to a physical person. With the term client we want to refer to the mobile device and the software, as in the traditional client/server sense.

3.9 Security Requirements

The following general security requirements [145] also apply to electronic banking systems:

- Confidentiality : ensures that only authorized entities have access to the content of the exchanged information. E.g., an eavesdropper should not be able to find out what transactions a particular user is executing.
- Entity authentication : users should be sure that they are communicating with the real bank, before sending sensitive information to it; banks should know the identity of a user before processing its transactions.
- Data authentication : i.e., data origin authentication and data integrity allows one to detect manipulation and replay of data, by unauthorized parties; data manipulation includes insertion, deletion and substitution. E.g., users and the bank want to be sure that the information they receive is genuine and fresh (not replayed).
- Non-repudiation : prevents an entity from denying previous commitments or actions. E.g., a bank should be able to prove to a third party that a user performed a certain transaction, in case that user denies having performed it.

3.10 Biometrics Authentication :

3.10.1 Biometric ID and Enhanced Transaction Security

There may also be a significant role for technology in improving mobile transaction security, as the following report makes clear. There has been a lot of work on biometric identity systems in recent years. The report surveys that work and assesses its relevance for mobile banking. In particular, it identifies a biometric technology approach that has already been incorporated in some mobile handsets—a sophisticated, but low-cost, fingerprint sensor. Use of this approach for mobile banking would work something like this: When a customer initiated a mobile banking transaction, the handset would request that the user register his or her fingerprint on the sensor, and the handset would compare the fingerprint to the one already stored in the phone (and, as a backup, also stored on the bank mobile transaction server). The handset would then send the transaction request and the result of the fingerprint comparison—in effect, a biometric ID authentication—to the bank server for approval and execution of the transaction. That would replace the device-based security safeguard (the SIM card) with something much more robust and harder to defeat. As the report makes clear, the technology to implement such a system is available now.

In summary, there is a confluence of technology trends leading to viable solutions that can enable very widespread access to financial services. Demonstration of these technologies and the related service models will help to accelerate commercial adoption, overcome regulatory hesitation, and empower the unbanked billions. We therefore invite widespread discussion of these solutions, in the belief that as they become better known, acceptance of mobile banking as a viable commercial enterprise by banks, telcos, and regulatory authorities will accelerate.

Biometrics is one approach to the authentication of an individuals claimed identity. Recognizing individuals through observation of particular physical characteristics is known as biometrics. A biometrics authentication is a two-stage process. During the first stage, some sort of capture device is used to take a measurement of particular physiological or behavioral characteristics and in the second stage; the measurement is compared to a stored value. Based on the comparison result the system makes an authentication decision. Biometric technologies do not actually compare the physical traits that they are designed to use as a unique identifier, rather, they create templates for comparison. This enrollment process may require the individual to provide multiple instances of the biometric trait. The initial comparison templates are created during an enrollment process. Figure 3.6 shows the diagrammatic representation of a biometric authentication system (Arumuga perumal, 2006)[146].

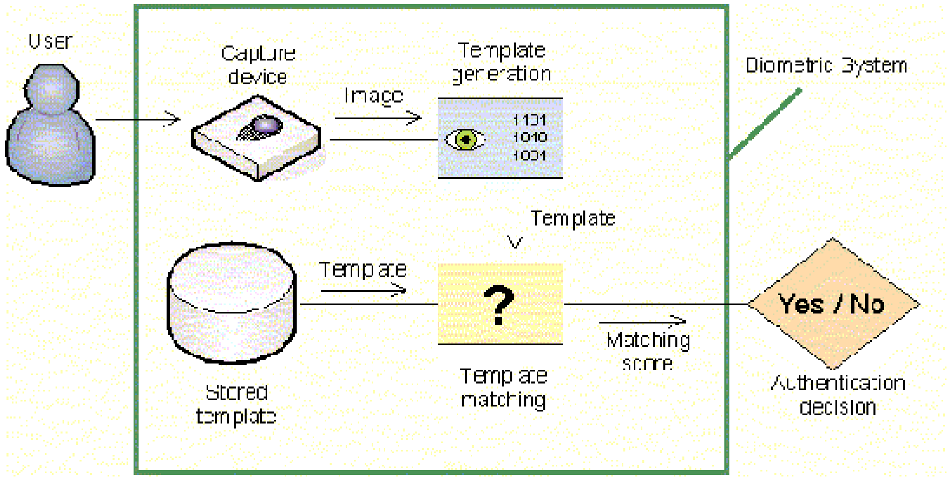


Figure 3.6 : Biometric authentication system

One way to increase the strength of an authentication mechanism is to use multiple factors of authentication. In the case of biometrics, this could involve requiring the user to input a password or PIN (Personal Identification Number) or to produce some sort of authentication token such as smart card that contains both the PIN and any one of the biometric systems with 1:1 matching. The advantage of such is that many are designed to operate with biometric systems and have sufficient space for storage of biometric templates with them. However, assessing the extent to which an additional authentication factor can increase the overall strength of the authentication services. When passwords are used for authentication, the decision is made relatively straightforward- if correct password is supplied the result is positive authentication, otherwise the individual is rejected. A biometric authentication is conceptually different, in that the decision is based on a probability. Any organization considering the use of biometrics needs to understand the impact of this when reaching a trust decision.

Biometrics is a measurable physical characteristics or personal behavioral trait used to recognize the identity or verify the claimed identity of an enrollee. Examples of physiological characteristics that are used in biometric device include fingerprints, the geometry of the face or hand and patterns within the iris or retina or in the layout of veins. Behavioral characteristics include voice pattern, gait and the dynamics of handwriting or keystrokes. For the authentication process the chosen characteristics must be unique to each individual. Also it is possible to measure the characteristics with the reasonable degree of accuracy. Once the measurement has been taken the data is converted into a biometric template. A template is a representation of the measurement that retains all the relevant information but takes up far less space than the original. It is this template that is compared to a template generated in the same manner during the initial enrolment procedure and based on the similarity of the two, a decision is made whether the user should be granted access.

Physical Biometrics are :

- Finger print -Analyzing fingertip patterns
- Facial recognition location - Measuring facial characteristics
- Hand geometry - Measuring the shape of the hand
- Iris Scan -Analyzing features of colored ring of the eye
- Retinal scan -Analyzing blood vessels in the eye
- Vascular patterns -Analyzing vein patterns
- DNA -Analyzing genetic makeup
- Biometric data watermarking is used to store/hide biometric information

Behavioral biometrics are :

- Speaker/Voice recognition system -Analyzing vocal behavior
- Signature/handwriting -Analyzing signature dynamics
- Keystroke/patterning -Measuring the time spacing of typed words

There are various biometric products like a plethora of fingerprint scanners, voice and facial recognition system, retina/iris scanners, hand geometry devices and signature verification systems available in the market.

3.10.2 The Biometric Process

Biometrics is typically defined as a means of uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Physical traits refer to what you are, as opposed to what you know, and include such things as fingerprint, face, retina, iris, hand geometry, and DNA. Behavioral traits reflect what you do, and include such actions as signature, gait, and keystroke. One biometric trait that is considered both physical and behavioral is voice. Regardless of the type of biometric that is used, the process involved when conducting biometric authentication is generally uniform. The user will first enroll them self in the system by providing multiple samples of the relevant biometric, which are then converted to digital, mathematical “templates” and stored for future reference. Once the user is successfully enrolled, they’ll gain biometric access to the system by presenting a “live scan” of the biometric trait, which is then compared to the reference template. The comparison of templates takes the form of either identification, which means that the live scan is compared to many templates to ascertain who the user is (aka a 1:N comparison), or authentication, where the live scan is compared to just one template to confirm that the user is indeed who they say they are (a 1:1 comparison). The determination of whether or not the two templates match will depend on the levels of accuracy demanded by the system administrator (the threshold level). This may seem oddly flexible for a security system, but in fact no biometric system is completely foolproof in returning a 100% total match. Rather the systems will indicate that the templates correspond to a certainty level of, say, 95%. It’s up to the administrator of the security system to decide how accurate they demand the match to be, and set the system accordingly via the threshold level. The distinction between identification and authentication is important when evaluating biometric systems, as the systems will require different threshold levels, not to mention vastly different storage and processing systems.

It’s also important to understand the different performance metrics of a biometric system, as these will impact what sorts of threshold levels are needed depending on the purposes of the security system. As their names imply, the False Match Rate (FMR, also known as the False Accept Rate, or FAR) measures the percentage of invalid users who are mistakenly allowed into the system, while the False Non-Match Rate (FNMR, or the False Reject Rate, FRR) measures the percentage of valid users who are mistakenly rejected by the system. While it would seem intuitive to set both measures as close to zero as possible, in reality there are tradeoffs made depending on the purposes of the biometric system. For example, access to a nuclear weapons site would demand absolutely no false matches, but will correspondingly result in a higher number of false rejections of valid users, which will then need to be resolved via other means of verification.

While military authorities will probably deem this type of inconvenience to valid users an acceptable price to pay for nuclear security, other organizations may demand more user-friendly systems for their employees or customers, say for access to an office building elevator or all-day passholders at a theme park. Because the levels determined for both FMR and FNMR involve a tradeoff in the system design, most scientists who are looking to compare biometric verification systems will in fact look at the level at which the FMR equals the FNMR, otherwise known as the Equal Error Rate (or EER). Other measures that are looked at when evaluating biometric systems are the times required for enrollment and verification, and the Failure to Enroll (FTE) rate, which would reflect how often users are unable to enroll at all due to any number of reasons, including illness and physical injury.

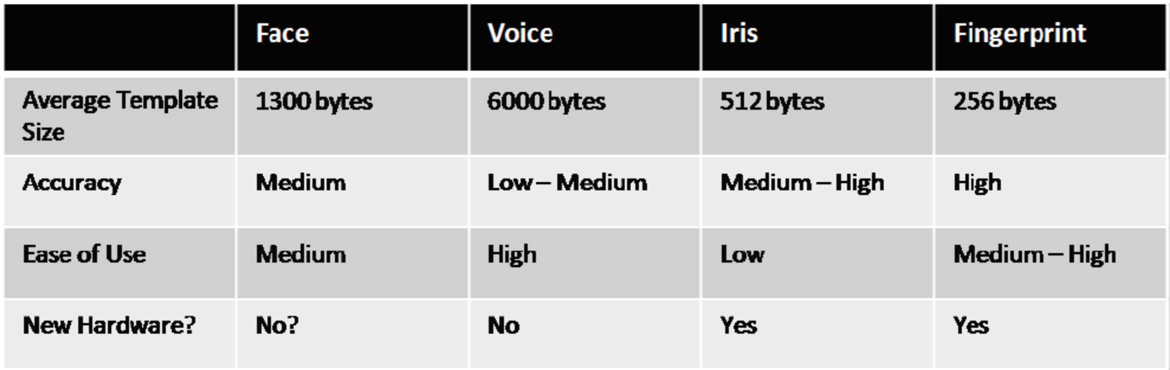
3.10.3 Fingerprints

The use of fingerprints to identify people has been around for over a century. It ’s the most mature biometric technology out there today, with accepted reliability and a well-understood methodology. As such, there are many vendors of fingerprint recognition on the market today, although not all of them employ compatible equipment or algorithms. Three of the traditional means of fingerprint recognition employ Optical, Captive Resistance/Pressure, and Thermal scanning technologies. While all three have been in use for years, with good reliability and accuracy, they do have weaknesses when faced with today's demand for better fraud prevention in the face of more sophisticated biometric applications, not to mention more sophisticated criminals. Specifically, all three of these types of fingerprint scanning can be defeated in various ways, such as using dead fingers or copying the last print used with adhesive film and re-presenting it to the scanner. Additionally, testing has shown that the elderly, manual laborers and some Asian populations are more likely to be unable to enroll in some of the traditional fingerprint systems.

A newer fingerprint technology, employing RF Imaging, uses ultrasonic holography of the outer layer of dead skin as well as the inner layer of live skin to create the template, rendering it nearly 100% accurate, not to mention resistant to the use of fake or dead fingers, or dirt and oil. In addition, the newer fingerprint systems use each new scan of the finger to enhance the existing template, thus making it more accurate with use over time.

While fingerprints have proven to be highly reliable and accurate over the years, particularly now using RF imaging, they're not completely infallible. They can be affected over time by such things as years of manual labor or physical injury, so there would probably be a desire to update the reference templates as and when necessary for commercial and financial applications. Other factors that can cause failure in a fingerprint scan are cold and humidity (particularly in the older types of fingerprinting), and location, angle and pressure of placement on the sensor (known as a platen). Other issues to consider are that the use of fingerprints requires physical contact, which can be a problem in some cultures, and the fact that fingerprinting's long association with criminal justice lends itself to some privacy resistance, although this will probably ameliorate over time with increased use of biometrics and updated privacy laws. Fingerprint capture technology is easily accommodated on a cellphone, with sensor sizes ranging from 12 mm x 5 mm to about 1.5 cm x 1.5 cm, and low power and processing requirements. The fingerprint template itself ranges in size from about 256 bytes to 500 bytes. Table 3.1 summarizes the main characteristics of the biometric technologies discussed.

Table 3.1 Main characteristics of biometric technologies.



	Face	Voice	Iris	Fingerprint
Average Template Size	1300 bytes	6000 bytes	512 bytes	256 bytes
Accuracy	Medium	Low – Medium	Medium – High	High
Ease of Use	Medium	High	Low	Medium – High
New Hardware?	No?	No	Yes	Yes

3. 11. Conclusion

To explore the bankers perspectives to introduce mobile banking as new distribution channel and Customers perspectives on mobile banking adoption, exploratory research design is identified as appropriate. The chapter contains an elaborative discussion on responsibility of banks while deploying online banking as new distribution channel through our new “modified customer equity approach model”. In order to explain the customer behavior of adapting mobile banking channel, we have proposed a new model called “Technology Acceptance based on Theory of Customer Stimulation by Education and Training for usage (TCSET). The new model is based on four constructs – perceived usefulness, perceived assurance, perceived ease of use, and perceived cost. These constructs stimulates the customers intention and behavior control to use mobile banking services. The various issues under, customer behavior and intention to use mobile banking transactions, like attitude, trust, convenience, perception, loyalty, privacy, security and comfort issues are discussed based on the developed model.

In this chapter, we also investigated the security threats in mobile banking implementations using the GSM network. The discussions support to build applications for portable devices that ensure users can securely send their banking information via the GSM network. The mobile banking solutions developed provide platforms for users to bank using SMS and GPRS. In order to enhance the security, biometric finger print detection can be used in mobile device. The possibility of using bio-metric finger print security to enhance user authentication are discussed.

Chapter IV

Results and Discussion

4.1. Introduction

The two prevalent online models in the banking industry are e-banks and e-branches. An e-bank is a banking institution that exists only on the Internet/mobile technology, with no bricks-and- mortar branch access. This framework gives a bank the opportunity to exist without paper, without geographical limitations, and without ever closing the doors to customers. The e-branch model is where a traditional bricks-and-mortar bank offers online banking to its customers. Some analysts believe that though e-banks are beginning to gain traction, it is still easier for a traditional bank to get existing customers to try online banking than e-banks to steal customers from bricks-and-mortar banks (Senior, 1999)[147]. In response to the increasing pressure by e-banks, many bricks-and-mortar banks have created independent e-bank subsidiaries. They have compelling reasons in support of creating independent e-banking units. First, in separating a online bank from the traditional structure, the slow moving corporate structure is replaced with an entrepreneurial one. Second, this approach gives the new unit much needed freedom from the traditional bureaucracy. Creating an autonomous online banking unit is in line with what many experts recommend when establishing business operations on the Internet. Success requires giving the electronic banking division independence, with separate management from the bricks- and-mortar part of the business. Third, this approach most effectively allows a so called "skunk-works" team to manage online banking by creating a group of innovative thinkers from existing business lines that report directly to the CEO (Leuchter, 1999)[148].

This chapter initially discusses the benefits of adoption of mobile banking as a new distribution channel by the traditional Banks and a study on business perspective of mobile banking is made by means of SWOT analysis. Various benefits of mobile banking from customer’s point of view are also discussed. This Chapter also deals with various mobile banking models and securities in financial transactions. In order to provide better security for financial transactions, a new mobile banking payment model called “Consumer oriented mobile business model” is proposed and discussed. The consumer oriented model allows customers to pay online for their shopping from their bank account using mobile devices. The business implications & advantages of “consumer oriented mobile business model” to decrease the possible frauds are also discussed and demonstrated for secured financial payment for online purchase. The secure SMS solution and the secure GPRS solution for the new model is also proposed which include secure SMS protocol and secure GPRS protocol. The security aspects of these solutions for the new model are also analyzed and discussed.

4.2. Business Implications

The business implications of mobile banking can be analyzed by knowing the benefits from bank's point of view, customer's point of view and by means of SWOT analysis of mobile banking. The driving force for online banking, in addition to convenience, is the low cost efficiency.

4.2.1. Benefits of online mobile banking from Banks' Point of view :

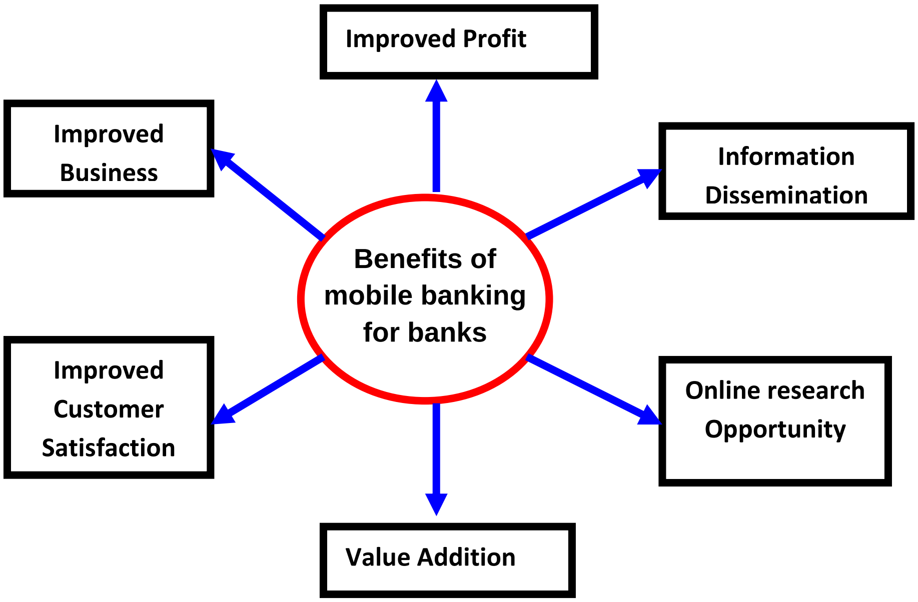

Improved Profit
Improved Business
Information Dissemination
Benefits of mobile banking for banks
Improved Customer Satisfaction
Online research Opportunity
Value Addition

Fig. 4.1 : Benefits of mobile banking from bank's point of view

1. Improved Business :

The first benefits for the banks offering mobile banking services is better advertisement, better branding and better responsiveness to the market. The banks which offer such services would be perceived as leaders in technology implementation and would enjoy a better brand image. It seems clear that partnerships between banks and service providers will become more common as different parties seek to develop cutting-edge abilities and services. Online mobile banking channel provides banks to adapt new technology and opportunity to new & innovative way of doing business. Cross selling using new online mobile banking is another opportunity to improves bank business.

2. Improved Profit :

The second benefits is in monetary terms. The main objective of every bank is to maximize profits and automated m-banking services from virtual office certainly offer a perfect opportunity for maximizing profits. Compared to the cost of setting up of branch offices in every city and every corners of the city and their maintenance, setting up of ATM's, the mobile banking services through virtual offices will be several thousand times profitable to the banks. On the fee side for different services, average payment in mobile bank costs 5 to 10 times less than payment in branch or using a teller machine. On the actual cost side, for the bank point of view, payment in online mobile bank cost 8 times less than payment in the branch due to improved operational effectiveness. Banks will also save a great deal of expense by reducing the number of employees in the bank and in closing some of the bank branches.

3. Value addition :

The third benefit is in terms of customer care and providing advertising information about value added services to the customers. Providing multiple distribution channels increases the value of the bank and its services in customers frame of reference and provides an opportunity to differentiate their products/services. Adapting new service distributing channel like online mobile banking improves the image of the bank in the industry sector. This will also improve the competitive edge of the bank and opportunity for global business expansion. The impact of information & mobile communication technology on value creation in any organization can happen either through increasing revenues at marginal cost, or through reducing costs at marginal changes in revenue, and thus enhancing operating profits.

4. Improved customer satisfaction :

By providing brick and mortar services at ubiquitous click and mortar, the customers can enjoy the advantage of technology innovations, the cost benefits of financial transactions and the quality of the services. This will improve the customer satisfaction and helps to retain the existing customers and attracts new customers towards the bank. Customer retention becomes ever more important. Research shows that the more services of his or her bank the customer uses, the higher the real and psychological switching costs will be. Also, the more services the customer uses, the greater are the bank's expected profits. Customer loyalty, therefore, gains importance over customer acquisition, and the value of customer relationship management becomes apparent.

5. Information dissemination :

Another important benefit is information dissemination. Some wireless infrastructures support simultaneous delivery of data to all mobile users within a specific geographical region. This functionality offers an efficient means to disseminate information to a large consumer population.

6. Online Research Opportunity :

Online Mobile banking facility provides considerable research opportunity to the customers before making financial decisions. They shop around for financial products, and make their own investment decisions – in part without consultants. Based on the data collected on customers decisions and other IT tools on data mining, banks can also do research on consumer behavior. This will help banks to take decision about various services. In developing countries, Researching via the financial services via mobile device is gaining importance.

4.2.2. Business Perspective of Mobile banking - SWOT ANALYSIS :

Managerial implications of mobile banking can be analyzed by SWOT analysis. A SWOT Analysis is an effective tool which can be used to examine the issues which will directly affect the success of alternative delivery mechanisms. For mobile banking transactions, the SWOT analysis is as follows :

Strengths :

- Customer access to information 24 hours per day.
- Timely access to information.
- The ability to offer a customer more than one method of retrieving information.
- Sophisticated technology systems will help to make a banking institute "future-proof."
- Diversity helps to capture different types of markets.
- The ability to cut internal costs due to advanced technology.
- Increased efficiency due to automation.
- Increased accuracy of banking transactions.
- Increased attractiveness due to new and convenient way of banking.

Weaknesses :

- High price of service.
- Continual altering of customer wants and needs.
- Hostile feelings of employees due to possible pending lay-offs due to automation.
- Multiple options for the customer.
- Initial investment in technology will be expensive.

Opportunities :

- The ability to obtain a larger customer base.
- Global expansion. This is an enormous market, which will be a great opportunity in the future.
- The ability to take advantage of the growing popularity of the mobile banking.

The future of m-banking and m-payments can be seen through three sets of eyes : the service providers, the retail consumers, and merchants.

Service providers

The key for service providers must be found in the business model. Banks do not want to be in a position of building systems to make the wireless operator rich through download fees of data supplied by the banks, whether this data originates from traditional banking or new products and services not yet invented. Telecommunication carriers do not want to be forced into the position of delivering low margin, price-sensitive commodity products. Mobile data services will be a viable and profitable business, and one day it will include mobile banking, but it will likely require the collaboration of both industries.

The business model could be based on a number of different approaches: transaction based, content based either by premium or by data volume, advertising, mobile spam, commission based, or part bundled. Whatever the case, one can expect that there will be many permutations and combinations before the various players find out what works. It can be also expect that what works will depend on the culture in which the service is imbedded.

Retail customers

When it comes to the Internet/mobile communication, what counts for users is speed, accessibility, reliability, desirable content, and effective services. It is expected that users will look to mobile data services for the same attributes. Mobile banking and mobile payment contribute very little to this equation, so the rollout of these services will depend on the evolution of other wireless products. The major short-term opportunities in m-commerce will be in compressing the supply chain and reducing administrative overheads in industry. Automating business-to business payment processes and integrating mobile technologies have direct cost-benefit potential and indirect potential to act as a pathfinder for retail m-banking.

Merchants

Obviously mobile payment and mobile banking have to be enabled on both sides of the transaction, including the merchant. In the short to medium term, credit/debit cards will prevail certainly in the country. As for the use of the mobile device to pay for vending machines purchases, this holds little attraction since vending machines typically deal with low volume sales of low value goods (Peffers, 2001)[149] and the penetration would have to be very widespread for this to work. It will be a long time before these organizations have to think about adapting their systems to accommodate more sophisticated mobile devices in the hands of consumers.

Threats :

- Continual changing technology.
- Uncertainty of the banking industry.
- Competition from "lower price" operations.
- Possible failure of products due to non-acceptance of customer.
- General competitiveness of the banking industry.
- Enhanced competition due to new entrants from mobile communication service industry.
- The fear of a lack of security is a higher hurdle to those mobile device users who do not use online banking than missing monetary incentives or insufficient comfort or functionality.

After reviewing this internal analysis, based on SWOT analysis, it can be suggested that the retail banking industry should diversity by adding this new technology. In the quantitative part of the study these propositions are tested through the focus groups and the general survey carried on bank managers and other employees.

Challenges

The key challenge for success will be aligning each of the following contributing factors until there is enough synergy to warrant m-banking :

- wireless access to compelling content;
- content evolution, including and especially premium material;
- communication technology, especially in terms of communication speeds and security;
- the device technology, especially the screen size and data interface; and
- the business model with better security for financial transactions and payment.

For those who have hopes of marrying m-commerce with marketing and merchandising, wireless will continue to leave a lot to be desired as a consumer experience. In the financial service industry, technology should not be confused with strategy. Leading-edge technology is one way to differentiate one organization from another, but implementing the technology in the absence of a clear business model is particularly risky. The early adopters of ATM technology certainly had a competitive advantage, but a competitive advantage based on technology is very difficult to sustain. Managers in virtually all industries understand that providing quality customer service is a key strategic component in firm profitability. The importance of service delivery and its impact on improving satisfaction and retention of customers, improving sales and market share, and improving corporate image can not be overstated (Lewis et al., 1994)[150]. Increasingly, one of the principal methods for making improvements in level of service individual firms provide their customers includes increased capital expenditures on service delivery technology. As with most other service providers, banks have moved quickly to invest in technology as a way of controlling costs, attracting new customers, and meeting the convenience and technical innovation expectations of their existing customers (Pyun et al., 2002)[151].

4. 2.3. Benefit from Customers Point of view

The benefit from the bank customers' point of view is accessing banking services at any where, any time and any extent of time. These features significantly save the valuable time of the customer. The main advantages of m-banking services for the Indian customers are as follows :

(1) Ubiquity : Through mobile devices, banking applications are able to reach customers anywhere at anytime. On the other hand, users can also get any information they are interested in, whenever they want regardless of where they are, through Internet-enabled mobile devices. In this sense, mobile business makes a service or an application available wherever and whenever such a need arises. Communication can take place independent of the users location. The advantages presented from the omnipresence of information and continual access to banking will be exceptionally important to time-critical applications.

Mobile banking, for example, can leverage this value proposition by providing alert notifications, such as for auctions, betting, and stock price changes, which are specified by the user as an important part of relevant personal content. As such, the real-time, everywhere presence of m-banking will offer capabilities uniquely beneficial to users. Banking services that are time and location sensitive, are likely to benefit from businesses exploiting this value-added feature of mobile banking.

(2) Personalization : An enormous number of banking information, services, and applications are currently available on the Internet, and the relevance of information users receive is of great importance. Since owners of mobile devices often require different sets of applications and services, mobile banking applications can be personalized to represent information or provide services in ways appropriate to the specific user. Additionally, personalized content is paramount in operating mobile devices because of the limitation of the user interface. Relevant information must always be only a single "click" away, since web access with any existing wireless device is not comparable to a PC screen either by size, resolution or "surfability". Therefore, subscriber profile ownerships is a key element in m-banking success, as it will allow selectively targeted m-banking applications. As such, the mobile database becomes a primary factor of m-banking success by compiling personalized data bases and providing personalized services. One example, is the SIM (Subscriber Identification Module) smartcards which serve as a mobile database allowing the user to run applications and operate secure transactions. Such personalized information and transaction feeds, via mobile devices, offer the greatest potential for the customization necessary for long-term success.

A value proposition is developed as superior consumer value is created through an increasingly targeted Internet experience for mobile users. For m-banking, the technological limitations magnify these value-for-time propositions. It has been estimated that every additional click-through, which a user needs to make in navigating through a commercial online environment with a mobile device, reduces the possibility of a transaction by 50%. Providing the user with the desired, most relevant information without forcing a complex click-through sequence will significantly improve the effectiveness of any mobile banking strategy. Value-for time propositions become maximized for those business strategies best able to implement m-banking distinguishing capabilities. M-banking will become differentiated from traditional e-banking based upon their abilities to integrate and actuate the advantages germane to mobile devices. Various applications may provide differing value for mobile Internet users.

(3) Reduced costs : This is due to availing and using various banking products and services by number of customers online. The transaction fee charged by banking service providers for financial services is much cheaper than conventional retail banking transaction fees. The heavy competition and the price war between mobile service providers also reduced mobile service usage cost.

(4) Flexibility : Because mobile devices are inherently portable, mobile users may be engaged in activities, such as meeting people or traveling, while conducting transactions or receiving information through their Internet-enabled mobile devices.

(5) Increased comfort : Many customers secretly hate their banks because of punitive charges, inconvenient opening hours and unhelpful branch staff. In mobile banking due to quick and continuous access, transactions can be made 24 hours a day, without requiring the physical interaction with the bank.

(6) Time saving : The main benefit from the bank customers' point of view is significant saving of time by the automation of banking services processing and introduction of an easy maintenance tools for managing customer's money. Since the response of the medium is very fast, the customer can wait till the last minute before concluding a fund transfer.

(7) Convenience : The ability and accessibility provided from wireless devices will further allow m-banking to differentiate its abilities from conventional banking and e-banking. People will no longer be constrained by time or place in accessing banking activities. Rather, m-banking could be accessed in a manner which may eliminate some of the labor of life's activities. For example, consumers waiting in line or stuck in traffic will be able to handle daily transactions through m-banking applications. Consumers may recognize a special comfort which could translate into an improved quality of life. One opportunity to increase value lies in m-banking capabilities that allow consumers to use banking services where they are not located. This ability to obtain information and conduct transactions from any location is inherently valuable to consumers. As such, m-banking offers tremendous opportunities to expand a client-base by providing value-added services to customers which is difficult to reach. By making services more convenient the customer may actually become more loyal. Consequently, communication facilities within m-banking are key applications for the delivery of convenience. Consumers will be looking for m-banking applications which can deliver functions like : sending and receiving e-mail, voice mail forwarding, document sharing, instant messaging; as well as transactional based activities.

(8) Better cash management : Mobile banking facilities speed-up cash cycle and increases efficiency of business processes as large variety of cash management instruments are available on internet sites of banks. For example, it is possible to manage companies short term cash via online or mobile banking like investments in over-night, short and long term deposits, in commercial papers, in bonds and equities, in money market funds etc. In mobile banking, customers can download their history of different accounts and do a what –if analysis on their own mobile device, before affecting any transaction on the web or through mobile service providers. This will lead to better funds management.

4. 3 M-banking Models

The business models for mobile banking may be based on Consolidation, Location based services, Immediate product payment, Bill payment, Systematic interoperability, and Non-credit card users. These models are based on specific applications. In consolidation model, the applications that provide consolidated financial views across institutions have value for those people who have banking relationships with more than one financial institution. Such an application would be able to consolidate all assets and liabilities in one view. Visual confirmation of such transactions is one of the attractive features of mobile banking and trading, as the user sees the complete transaction all at once. The restricted screen size of mobile devices is a challenge for this type of visibility, certainly in the near future. In Location-based services model the mobile technology is adopted for identifying and using the actual physical location of the user. This provides an opportunity to customize both data and services by taking into account personal factors and location-related factors (Hightower & Borriello, 2001)[152]. Currently, providing and using location-specific information is possible with a wireless device. The costs and benefits of this functionality to all of the parties involved and the risk that users may be reluctant to have their movements recorded in this way. In Immediate product/service payment model, mobile devices afford the opportunity for consumers to purchase goods or services and draw the payment directly from their bank accounts in a manner similar to the debit card. Bill payment model allows payment bills online. One of the arguments that favor the use of a wireless device in many situations is to satisfy the need for urgency. A cell phone is often invaluable in the case of emergency, which is by definition urgent and time sensitive. Generally, there is not much urgency or time sensitivity to bill payment transactions or most other bank transactions, with the possible exception of the minority of investors who are active traders (Kiesnoski, 2000)[153]. Consumers always look for uninterrupted service with an uncomplicated interface between the customer, the device, the wireless service, the network, the merchant, and the bank. This systemic interoperability is a key user consideration in systematic interoperability model. M-banking does offer the potential for a portable payment/banking system that provides systemic interoperability. Presently in most of the countries, the payment mechanism of choice for medium-sized payments is the credit card. Under Non-credit card users model, Mobile banking and mobile payment schemes would have value for those people who do not have a credit card, such as the teenagers, children, or poor credit risks. If this functionality is delivered through facilities developed by the telephone companies, which will aggregate charges onto the telephone bill, the technology could actually contribute to the disintermediation of the banking industry. Banks could, of course, offer a similar micropayment aggregation function. There is some question of which industry is best positioned to do this. Is it the organization with the close connection to the customer's bank account or the organization with the close connection to the communication network ?

4.3.1. Consumer Oriented New Model :

(Our Model on Secured Transaction for Ubiquitous Banking)

The emergence of mobile banking will increasingly be intertwined with the emergence of mobile commerce and mobile payments. M-banking, rather than driving m-commerce, will in fact be driven by the increasing availability of mobile-focused, user-friendly content. And because the rise of m-business will be based on the inclusion of a strong payments engine, which can provide better payment transaction processing services.

Regardless of the bright future of mobile banking, its prosperity and popularity will be brought to a higher level only if information can be securely and safely exchanged among end systems (mobile users and banking service providers). Online banking through mobile service providers is more secure than online banking through internet because of the usage of private network of the service provider (PNSP) and the users' personal mobile device. The existing electronic authorizations for mobile payment security are based on account - holder authentication by the payment system. The use of secure and convenient mobile personal devices through PNSP could revolutionize the payment, banking and investment industries worldwide.

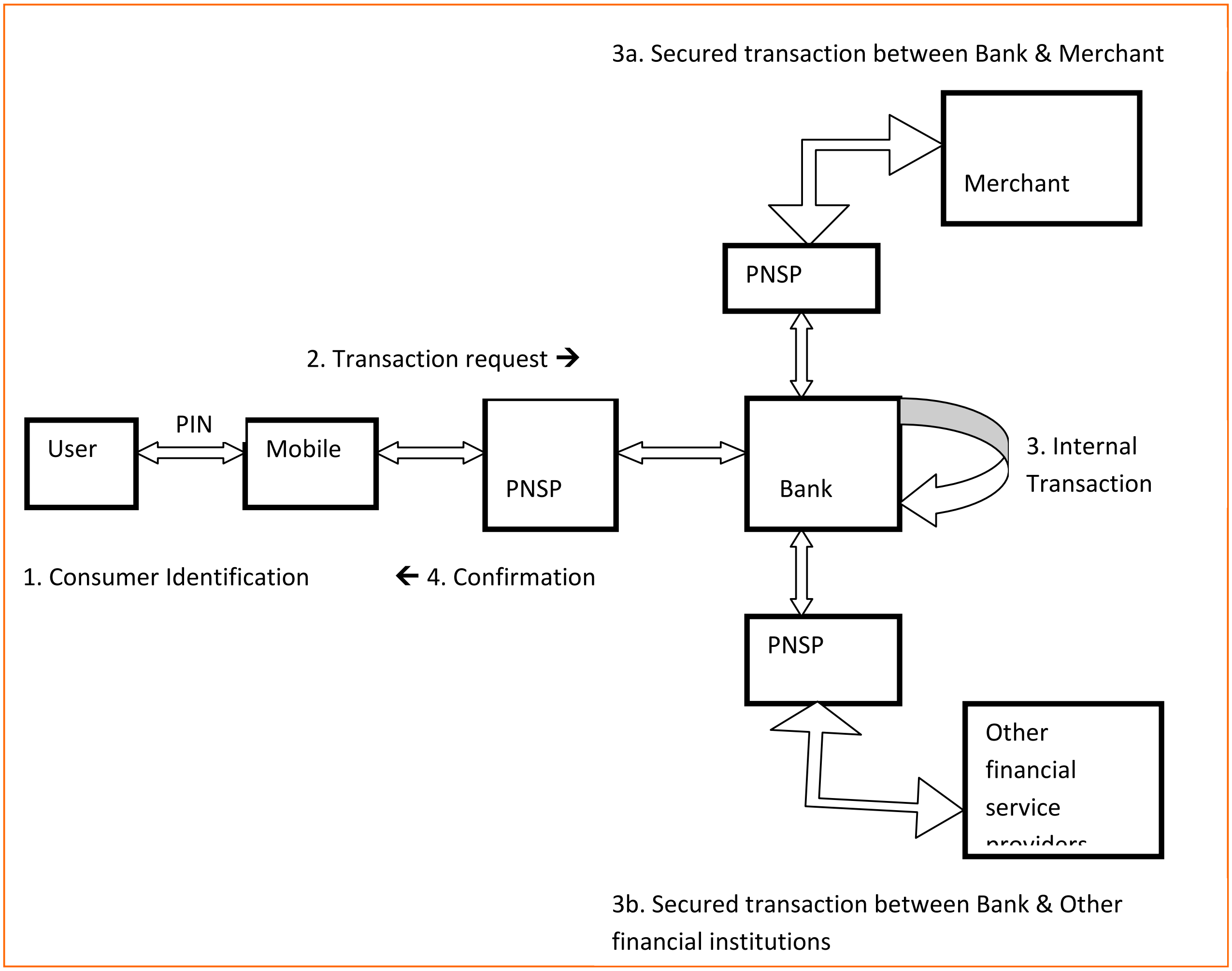

3a. Secured transaction between Bank & Merchant
Merchant
PNSP
2. Transaction request →
PIN
User
Mobile
PNSP
Bank
3. Internal Transaction
1. Consumer Identification
← 4. Confirmation
PNSP
Other financial service providers
3b. Secured transaction between Bank & Other financial institutions

Fig. 4.2 : Consumer oriented model - uses Private Network Service Provider for enhanced security.

In consumer oriented model proposed in this paper (Fig. 4.2), the mobile banking services are provided through mobile network service provider PNSP, either by collaboration or by strategic alliance. A consumer can use any private mobile network to access a particular real or virtual bank.

The consumers and businesses in emerging markets are likely to find mobile financial services more attractive than do their counterparts in developed markets, because they have fewer alternatives. For many remote or low-income consumers, mobile handsets and the mobile Internet could for the first time provide access to financial services such as basic banking and electronic payments; otherwise financial-services providers find such segments impossible to serve cost-effectively. Mobile networks are cheaper to build than fixed-line networks, and mobile services are generally cheaper to roll out than their precursors. A mobile-payments network, for example, can cost less to create and operate than an electronic point-of-sale (POS) merchant network. This means that some countries will be able to leapfrog over intermediate technologies and move directly from a paper-based payments system to a mobile one, without ever having to build an extensive wired POS or automated-teller-machine network.

In this model, based on user request, the device identifies the user through physical possession of mobile phones, passwords, or biometrics such as voice recognition (path 1). The mobile banking service provider authenticates the transaction request from the device via either subscriber identification (as with existing phones) or cryptographic mechanisms such as digital signatures or secure protocols, like the Wireless Transport Layer Security Specification through private network service provider PNSP (path 2). The users can perform secured operations on account balance or loan account statement, transfer money between two accounts in the same bank (internal transaction), loan payment, or payment of electricity, water, phone, credit card and cellular phone/pager bills, through the bank (path 3). The financial transaction can be also performed between the mobile banking service provider, and the merchant for m-commerce payment through PNSP (Path 3a) and/or other financial institution(s) for bill payments or interbank transfer through PNSP (path 3b) and may involve secure payment protocols such as Internet Keyed Payments/Secure Electronic Transactions, or iKP/SET (MacGregor, 1997)[154]. After completion of requested transaction, the mobile banking service provider delivers a confirmation of transaction to the user (path 4).

In today’s mobile phones, authorization is via subscriber identification mechanisms, which do not provide non-repudiation. However, in future, mobile consumers might also use a secure mobile signing device, to avoid disputes. This device may allow high-value transactions, as well as paying mobile operators who are not completely trusted (such as when roaming). Mobile communication mechanisms (such as GSM) allow the foreign (visited) network to authenticate the user with information from the home network. Charging requires prior agreements between the visited and the home networks. Designers of the Universal Mobile Telecommunications System (UMTS) recognized the difficulty of establishing agreements in advance among visited networks and all home networks (Horn, and Preneel, 1998)[155]; thus, UMTS includes mechanisms for dynamic negotiation and setup of roaming agreements between a visited network and a home network. Roaming agreements seek to establish fees and ensure operator trustworthiness.

Operators are trusted to deliver payments in time; foreign (remote) operators are also trusted to not overcharge visiting customers. A secure signing mobile device can prevent fraud (overcharging) by foreign network providers, thereby allowing more automated and variable roaming agreements. Operators can also use the Final Payments protocol, (Herzberg, 2003)[156] to extend pair-wise trust relationships into global trust relationships, allowing automated, secure, low-cost universal roaming.

Other payment scenarios involve mobile service providers participating in the payment transaction itself, not just in its authorization. One motivation is to establish new payment networks, possibly involving mobile operators and financial institutions as providers of mobile payment services. Motivations for establishing new payment networks include the exploitation of business opportunities inherent in the billing, customer-service, and technical relationships among mobile users (and devices) and mobile operators. Another is support for low-value payments (micropayments) and final (irreversible) payments, each possibly yielding additional mobile communication services. Micropayments and final payments using mobile devices may enable the purchase of content and services delivered via the network, as well as person-to-person payments and money transfers; the latter represents a substantial opportunity, especially in light of the millions of overseas employees worldwide. Moreover, due to their ability to allocate responsibility for fraud, these new payment networks may lower the cost of transactions (as a percentage of the transaction) for large-value payments and money transfers. In other case, the mobile service provider is part of an existing payment network. In either case, the mobile provider acts on behalf of the user as a wallet server, as it is located along the route between mobile device and bank. The mobile service provider may implement a variety of payment protocols, ranging from the complex (such as iKP/SET) to the simple (such as SSL/TLS transmission of credit card numbers). The mobile network service provider may securely inform the bank of any pending transaction, allowing them to reject fraudulent transactions.

To avoid lack of security and a high level of fraud which is a major obstacle to people embracing the possibilities and advantages of using internet based online banking services, in this model, it is proposed to use the secured network provided by mobile network service providers. The integration of present mobile communication technology with banks is an ideal solution to increase the potential customers trust towards ubiquitous financial transactions using mobile devices. This model supports the user identification through physical possession of mobile device, passwords, or biometrics and authenticates the transaction request from the device by mobile banking service provider through mobile network service provider via either subscriber identification or secure protocols, like the Wireless Transport Layer Security Specification. The secured financial transaction is performed by the mobile banking service provider, with the help of the network service provider(s) for financial transactions as well as for bill payments. The transaction process is completed by delivering a confirmation of transaction to the user. Such consumer oriented model changes the attitude of customers towards using m-banking services due to the advantages of convenience, low cost, any where, any time banking and increases trust on online financial transaction.

How much value a mobile-financial-services business can create depends largely on its relevance to a given market. But in any market, a business can create value in two ways: directly, by enhancing benefits to customers or reducing costs for participants, or indirectly, by increasing cross-selling, cutting the cost of acquiring customers, or reducing customer churn. Indirect benefits are available only to the provider that comes first to market with a given service or that has assets or capabilities distinctive enough to retain share once competitors have entered the market.

The low-cost mobile banking can bring into the fold a considerable group of consumers who formerly could be served only at too high a cost. It replaces the most costly elements of a basic banking service (ATMs and tellers) with a deposit and withdrawal process that relies on much cheaper mobile communications and "franchised" (merchant-based) tellers. But the mixing of brand names, distribution networks, and financial services is leading to complex ownership and alliance structures, and extensive vertical integration could undermine competition. Links can lead to fewer benefits for consumers when they exploit reputation or involve sunk-cost investment to reduce competition on price. Mixed conglomerate structures can also challenge a basic principle of competition policy, the separation of content and carriage. Some mixed conglomerates-such as a telecom company merged with a financial service provider-will be able to control content and carriage and can limit access to networks by buyers of services, or to suppliers that wish to access potential customers. Lack of competition may not result in higher prices for financial services, but it could reduce product and process innovation. To ensure competition and innovation, restrictions may be called for on such vertical or horizontal links. In considering such restrictions, authorities will have to balance many issues, including the potential risk diversification benefits of mixed conglomerates and the benefits for competition of entry by non-financial entities in the financial service sector.

At present, banks, for the most part, are watching from the sidelines while their primary role as the premier financial intermediary is being diminished by online brokers and other financial service providers. As recently as two years ago, many leading banks were preoccupied with merger and acquisition aimed at expanding networks of brick-and-mortar branches rather than creating or pursuing virtual branches in cyberspace. In truth, bankers' main motive to implement Internet banking was, and still is, to prevent the defection of their customers to other electronic banks or other financial service providers. Such consumer oriented model changes the attitude of customers towards using m-banking services due to the advantages of convenience, low cost, any where, any time banking and increases trust on online financial transaction.

4.3.2 Analysis of the model:

In a mobile setting, the customer’s interactions with the merchant, the bank, service provider, network operator and other intermediary entities may involve different service channels such as SMS, WAP, data and/or voice delivery mechanisms. The purchase interaction with the merchant, access to the bank to effect a payment, the authentication process and execution of the payment transaction may involve multiple steps, distinct delivery channels and separate time segments.

Wireless technologies are characterized by a variety of carriers, service bearers, delivery channels, application functionalities, communication protocols, device capabilities and security attributes. Frequently, they coexist in parallel and are incorporated into systems and networks to provide accessibility and reciprocity between different participants and entities. The authentication process usually requires an exchange of data between the customer, the merchant and the bank (or the payment service provider). This usually entails several steps comprising a challenge and response interaction, and possibly offline confirmatory notifications subsequently.

In this model, based on user request, the device identifies the user through physical possession of mobile phones, passwords, or biometrics such as voice recognition. The mobile banking service provider authenticates the transaction request from the device via either subscriber identification (as with existing phones) or cryptographic mechanisms such as digital signatures or secure protocols, like the Wireless Transport Layer Security Specification through private network service provider (PNSP). The users can perform secured operations on account balance or loan account statement, transfer money between two accounts in the same bank, loan payment, or payment of electricity, water, phone, credit card and cellular phone/pager bills, through the bank.

The financial transaction can be also performed between the mobile banking service provider, and the merchant for m-commerce payment through PNSP and/or other financial institution(s) for bill payments or interbank transfer through PNSP and may involve secure payment protocols such as Internet Keyed Payments/Secure Electronic Transactions, or iKP/SET [157]. After completion of requested transaction, the mobile banking service provider delivers a confirmation of transaction to the user.

Use of this approach for mobile banking would work something like this: When a customer initiated a mobile banking transaction, the handset would request that the user register his or her fingerprint on the sensor, and the handset would compare the fingerprint to the one already stored in the phone (and, as a backup, also stored on the bank mobile transaction server). The handset would then send the transaction request and the result of the fingerprint comparison—in effect, a biometric ID authentication—to the bank server for approval and execution of the transaction. That would replace the device-based security safeguard (the SIM card) with something much more robust and harder to defeat.

In today’s mobile phones, authorization is via subscriber identification mechanisms, which do not provide non-repudiation. However, in future, mobile consumers might also use a secure mobile signing device, to avoid disputes. This device may allow high-value transactions, as well as paying mobile operators who are not completely trusted (such as when roaming). Mobile communication mechanisms (such as GSM) allow the foreign (visited) network to authenticate the user with information from the home network. Charging requires prior agreements between the visited and the home networks. Designers of the Universal Mobile Telecommunications System (UMTS) recognized the difficulty of establishing agreements in advance among visited networks and all home networks [158]; thus, UMTS includes mechanisms for dynamic negotiation and setup of roaming agreements between a visited network and a home network. Roaming agreements seek to establish fees and ensure operator trustworthiness.

Operators are trusted to deliver payments in time; foreign (remote) operators are also trusted to not overcharge visiting customers. A secure signing mobile device can prevent fraud (overcharging) by foreign network providers, thereby allowing more automated and variable roaming agreements. Operators can also use the Final Payments protocol, to extend pair-wise trust relationships into global trust relationships, allowing automated, secure, low-cost universal roaming.

There are two scenarios in which the customer's bank account can be debited for payments. The first is where the customer is authenticated by the bank in order to enable the customer to access his account online to effect a payment. In the second scenario, the customer authorizes a third party to raise a debit against his account. The customer also informs the bank about the arrangement and seeks its approval to accept such debits against his account by a third party. This may occur when the customer makes use of bill payment functions provided by a third party. Another way this can occur is when a merchant or a payment service provider switches the customer to his bank so that he may directly effect a payment transfer from his account to that of the other party.

In all cases, the bank must authenticate its own customer before allowing him access to his own account. The bank should not allow nor rely on third party authentication of the bank's own customer.

Public Key Infrastructure

Public Key Infrastructure (PKI) assures "Confidentiality", "Authenticity" and "Integrity" of the information which 2 or more members exchange. The PKI relies on Public Key Cryptography and hashing techniques.

Secure Communication between Customer and Service

In present deployment of PKI, it's able to secure the communication so that no one can sniff the information passing on wire. Digital Certificates are issued only to servers, i.e., clients can authenticate the servers, but the servers authenticate clients using Usernames, Passwords and Bio-metric identification technique.

In case of web based transactions, SSL (Secure Socket Layer – uses PKI) allows the client to interact with server in a secure fashion, but it's the web browser who authenticates or rather trusts the server by using the trusted root certificates that already come with web browsers. Here the user may or may not be aware of what these certificates are and who has put them in his browser or machine etc. In a way its like web browser software, which is taking decision on behalf of user.

The current SSL and Internet Security architecture doesn't provide any non-repudiation mechanism, as what happens at the server or service while transacting is unknown to anyone. SSL only protects the channel communication by encrypting the data before transfer. Once it is transferred to the server, the data would be in the hands of the service (or the service provider), which can tamper the information or misuse.

Customers need to be assured that their financial information is secure, and that wireless transactions are safe. The mobile business service should improve its reliability and stability by providing comprehensive technical and operational support to give users positive experiences and increase their satisfaction, and thus enhance the service provider's reputation and build customers' loyalty.

4.4 Secure SMS Solution Using new model through Biometric Authentication

The solution provides a secure messaging protocol that uses SMS. The secure messaging protocol overcomes the existing security shortfalls in the GSM architecture using biometric authentication. The messaging protocol has been integrated with mobile banking system so as to improve the security of SMS banking. For demonstration purposes, three types of transactions have been simulated in this project. These transactions are: check balance, transfer money and purchase airtime. The types of transaction can change depending on the types of services provided by the bank.

4.4.1. Secure SMS Protocol

1. Message Structure

The secured SMS message is divided into multiple fields to accommodate for the various security checks required for the protocol. To ease the understanding of the message structure, Figure 4.3, shows the structure overview for a secure SMS message. The numbers above the fields are the minimum number of bytes required for each field in the message. The number of bytes for each field can be increased depending on the implementation requirements.

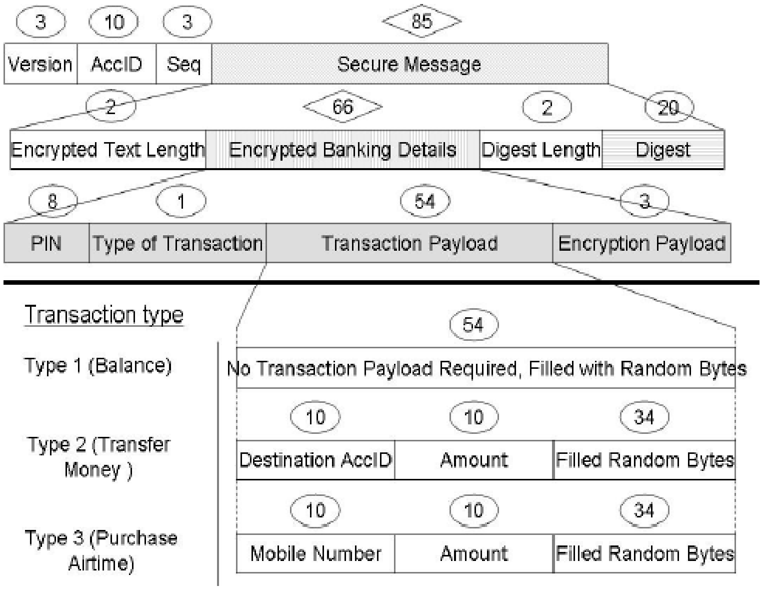


Figure 4.3 The Structure of a Secure SMS Message

The use of each labelled structure is explained below:

The *Version* is the mobile application version number. It contains a specified bytes pattern. The receiver checks if the first three bytes of the received SMS message are valid for the bank application. If the message version number does not match the application version, then the message is discarded. As there are possibilities that the server can receive accidental SMS messages that are not intended for the bank server. The usage of the version bytes is to help to eliminate these erroneous messages.

The *AccID* contains the bank account identifier of the user.

The *Seq* is the user s current sequence number of the one-time password.

The *Encrypted Text Length* contains the number of next bytes that are the ciphered message.

The *Digest Length* contains the number of next bytes that contains the message digest.

The *Digest* contains the calculated digest value of the message. The use of the digest is for the server to check for message integrity. For the secure SMS banking protocol, a single digest of the following fields is calculated: *Version*, *AccID*, *Seq*, *PIN*, *Type of Transaction* and *Transaction Payload*.

The content of the following fields is encrypted using the generated session key.

The *PIN* contains the user predefined password. This is used by the receiver application to authenticate the user.

The secure SMS message can be used for different types of transactions. The *Type of Transaction* is used by the bank server application to identify the type of transaction it should perform.

The *Transaction Payload* is the extra data that is used for a transaction, but it is not used for any security purpose. The content of the Transaction Payload depends on the type of transaction requested. The structure of the payload depends on the type of transaction offered by the bank.

2. Protocol Sequences

In the GSM network, SMS messages are sent asynchronously to the receiver, because of this the Secure SMS protocol is asynchronous. The figure below illustrates the overview of the secure SMS protocol.

We can consider the Secure SMS protocol to be divided into two parts. The first part is the message generation. The mobile phone generates the message and sends it to the server. The second part is the message security checks. The server reads the received message, decodes the contents and performs security checks. The following subsections describe each part of the protocol.

3. Generating and Sending Secure SMS Messages

The mobile phone captures all the required security information from the user. This information is used to generate the secure SMS message to be sent to the server. The mobile application has
a preset version bytes pattern, this pattern is inserted into the message. The message hash value a number which can ensure message integrity for the receiver side. The requirement of maintaining the message integrity is that at least some of the contents that are used for calculating the message digest need to be encrypted. This can ensure message integrity because if the message is intercepted, the attacker cannot use the encrypted contents to generate another digest. The integrity validation will not pass if any part of the original message is altered. The fields of content that need to be encrypted are dependent on the needs of the developer. The protocol requires that the message to have some identification details not to be encrypted. This is for the receiver to identify the account holder s identity. The algorithm used for encryption must be a symmetric encryption algorithm. The key used for encryption is generated from the one-time password entered by the user. The one-time passwords are only known by the server and the user. After the application completes processing the security contents, the contents are placed in the SMS message according to the message structure described in the Message Structure section. The SMS message is sent to the server via the GSM network.

4. Receiving and Decoding Secure SMS Message

When the server receives the message from the cellular network, it breaks the message down according to the structure described in the Message Structure section. The server first checks for the version bytes pattern. If the version is correct, it is assumed that the message is suitable for the secure SMS protocol. Next, the server reads the account identifier from the message and checks if the account identifier exists in the server database. After this, the server retrieves the current sequence number for the given account identifier. The server checks if the sequence number read from the message matches the sequence number read from the server s database. If the above security checks all passed, the server proceeds to retrieve the one-time password from the database. The password is indexed by the account identifier and the sequence number. Thereafter the server uses the retrieved password as the decryption key to decode the encrypted contents. If the decryption is successful, then the used one-time password is discarded and the server s sequence counter for that account gets incremented by the value of 1.

After the decryption, the server reads the secure contents that are required for the calculation of the message digest. The message digest is calculated using the same algorithm as the algorithm used by the mobile application. The server compares the two digests for message integrity. If the message is proven not to have been altered, then the server retrieves the PIN (the account holder s personal password) from the message and compares it against the account holder s PIN from the server s database. If all of the above security checks pass, the server performs the requested transaction.

4.4.2 Security of the Secure SMS Protocol for new Model

The following subsections describe how the Secure SMS protocol conforms to the general security requirements.

1. Confidentiality

This is achieved by encrypting the message using a symmetric secret one-time password. The one-time password is only shared between the user and the bank server. The strength of the confidentiality depends on the security strength of the passwords generation algorithm used and the strength of the ciphering algorithm used. It is assumed that only the authorized user will know his/her list of passwords and the passwords are never shared with other people.

2. Integrity

The message digest is the hashed value of the message content calculated server application and the mobile phone application. If the content is altered during transmission, the hashing algorithm will generate a different digest value at the receiver side. If the digests mismatch, the receiver will know that the integrity of the message has been compromised. The strength of the integrity checks depends on the strength of the algorithm used to generate the digest value and it also depends on the strength of the encryption algorithm used to hide the confidential data.

3. Authentication

For the receiver to authenticate the user, the user must provide his/her authentication detail(s) to the receiver. This authentication process is performed by validating the message PIN with the receiver stored PIN. The PIN is previously selected by the user when the user registers for a mobile banking account. The strength of the authentication depends on the password selection strategies used.

4. Non-Repudiation

Only the account holder and the bank server are supposed to have the one-time password. The bank server does not generate the same one-time password more than once. Therefore every onetime password is unique in the server s database. Each pair of one-time password and sequence number is only allowed to be used for a single user. Therefore the user cannot deny not sending the message because only that specific user has that unique pair of password and sequence number to encrypt the message. If the bank server can use the same sequence-password pair to decrypt the message, then it indicates that user must have sent the message.

5. Availability

The availability of this protocol depends on the availability of the cellular network. The time it takes for a message to be delivered depends on the density of network operator base towers. The number of transactions that the server can handle at once depends on the hardware capability. If the server s hardware can handle multiple incoming messages then the server can perform multiprocessing to accommodate for more requests. The protocol has no restriction on the type of hardware needed. Therefore it is up to the developers to decide the hardware specifications.

4.5 Secure GPRS Solution for new model through Biometric Authentication

In order to rectify the security problems mentioned above, two solutions were proposed. The first solution extends the security features in the present WAP implementations using biometric authentication and the second solution is a completely new GPRS security protocol.

4.5.1 Extension of present WAP implementations

To provide the bank with full control of the WTLS protocol, this solution lets the bank customers connect to its bank network through a customized WAP gateway which operates in its network realm[159]. The customized WAP gateway disallows the following handshake options:

☛ Abbreviated handshake

☛ Server authenticated full handshake

☛ Anonymous key exchange suites

4.5.2 New Secure GPRS protocol

The Secure GPRS protocol is a tunneling procedure that has been designed to take care of security in M-commerce applications. We have used this protocol to create and conduct secure connections between mobile devices and the bank servers. The Secure GPRS protocol consists of two main components; an initial client server handshake and the transfer of data packets (SGP record protocol) using the created secure tunnel and exchanged cipher suites. The SGP protocol uses some principles of pretty good privacy (PGP) as described in [160].

1. Protocol message components (Message Structure)

Each SGP message sent between the client and server has 3 components i.e. the message timestamp, message, and the message type. The message timestamp is used by both the client and server to prevent replay attacks, and the message type is also used by both the client and server to identify the message sent. Figure 4.4 below illustrates this message structure.

Error message

Handshake message

Go-Ahead message

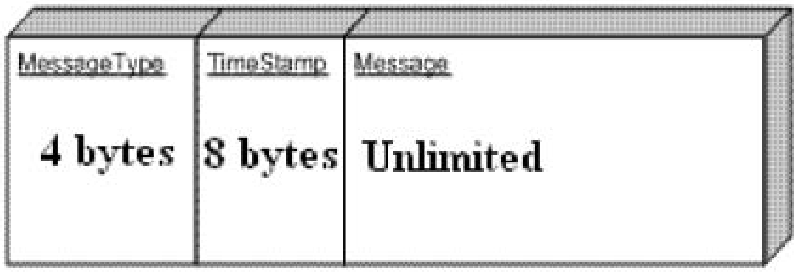


Figure 4.4.Structure of message sent

2. Client Protocol Initialization

When a client starts-up the mobile application a one time 512 bits RSA key pair is generated. Once the keys have been generated the client sends its public key to the server. These keys are used in the protocol to create digital signatures for the client. These digital signatures are verified by the server using the sent client public key; this authenticates the messages sent by the mobile client. To complete the client protocol initialization the client generates a PBE AES session key using the client s password.

3. User Authentication

The authentication takes place in two different sections; the first authentication is done by the mobile device and the second by the bank. When a user registers to use the banking service a server certificate signed using the client s password is included as part of the application. This certificate is used to authenticate the account holder on the phone. When a user enters a password the phone application generates an AES key using this password. Using this key the application attempts to retrieve the server s public key in the server s certificate, if the server s public key is retrieved successfully the initial client authentication is complete; else the client is asked to re-enter the password. Importantly the client is only allowed three login attempts; if the login fails in the three attempts the account is blocked. The second user authentication is done by the server; the client sends its encrypted client account ID. The server then gets the password from the database and recreates the AES key; if it can successfully decode the encrypted message then the client is authenticated.

4.5.3 Security of the Secure GPRS Protocol

The following subsections describe how the Secure GPRS protocol conforms to the general security requirements.

1. Confidentiality

This protocol has been designed to take care of the core banking security requirements. It ensures confidentiality of data between the bank and the mobile application through the use of AES encryption and one time session keys.

2. Integrity

In order to ensure integrity of data being communicated the protocol detects any changes made to the data on its way to either the bank server or mobile application through the use of RSA digital signatures.

3. Authentication

The protocol ensures both client and server trust and authenticate each other prior to sharing sensitive information. Mutual authentication is established by the use of SGP (Secure GPRS Protocol) certificates. Each mobile application is packed with the server s certificate, in this certificate there is the server s public key. This public key is used to authenticate the server. The server also uses the client s SGP certificate to authenticate clients.

4. Availability

In order to avoid replay attacks the bank server detects stale messages by checking the timestamps in each message it receives.

The Secure GPRS Protocol is an abstract protocol which has been designed to run on any platform and can be implemented in any programming language.

4.6. Conclusion

The business implications of benefits of adoption of mobile banking as a new distribution channel by Banks, business perspective of mobile banking by means of SWOT analysis, and various benefits of mobile banking from customer’s point of view are discussed. Various mobile banking models and securities in financial transactions are discussed based on the basis of variations in dimensions, and technological knowledge. In order to provide better security for financial transactions, a new mobile banking payment model called “Consumer oriented mobile business model” is proposed and discussed. The consumer oriented model allows customers to pay online for their shopping from their bank account using mobile devices. The business implications & advantages of “consumer oriented mobile business model” to decrease the possible frauds are also discussed and demonstrated for secured financial payment for online purchase. The secure SMS solution and the secure GPRS solution for the new model is also proposed which include secure SMS protocol and secure GPRS protocol. The security aspects of these solutions for the new model in terms of *Confidentiality, Integrity, Authentication, and Availability* are also discussed. To enhance the security for financial transaction a biometric authentication system is proposed. Use of this approach for mobile banking would work something like this: When a customer initiated a mobile banking transaction, the handset would request that the user register his or her fingerprint on the sensor, and the handset would compare the fingerprint to the one already stored in the phone (and, as a backup, also stored on the bank mobile transaction server). The handset would then send the transaction request and the result of the fingerprint comparison—in effect, a biometric ID authentication—to the bank server for approval and execution of the transaction. That would replace the device-based security safeguard (the SIM card) with something much more robust and harder to defeat.

Chapter V

Summary and Conclusions

5.1 Introduction

The dramatic increase in the use of mobile phones has been closely followed by the increase in mobile fraud. Although eager to use mobile financial services, many subscribers are concerned about the security aspect when carrying out financial transactions over the mobile network. In fact, lack of security is seen as the biggest deterrent in the widespread adoption of mobile financial services. Hence, fraud prevention has become an essential ingredient in the success of online financial transactions.

In this study, it is found that proper education and training (awareness) on mobile banking services and their security will certainly enhance the usage of mobile banking facility by banking customers. Banks have to plan proper strategy to provide mobile banking distribution channel, to attract existing and new customers to this new distribution channel, to decrease the cost of their business and to provide better service at low cost to the customers along with other advantages. TSCET model on mobile banking is proposed. A new business model is developed in order to accelerate the financial transaction process and to provide Value added Services to the customers. This consumer oriented model allows customers to pay online for their shopping from their bank account using mobile device. To enhance the security for financial transaction a biometric authentication system is proposed.

5.2 Summary of the Project

In the first chapter of the report, an overview of opportunities and challenges for mobile business is given. This includes various value propositions, implications of mobile devices, implications of mobile networks, mobile business value chain, advantages of mobile business over e-business, mobile business activity including value added applications, legal concerns and implications to applications and service providers. The chapter also contains information about mobile banking models, services, technologies, payment methods, and securities of financial transactions.

In the second chapter, an overview of past, present, and future mobile banking technologies is presented. This includes review on mobile communication technology, information exchange technology, location identification technology, and security considerations. The chapter also contains an overview of mobile communication devices. Technological aspects of various mobile payment technologies are also discussed with their advantages and limitations. Literature review on the various research issues like Online banking, Significance of mobile business activity in financial sector with special emphasis in banking sector, and Security issues on mobile banking transactions are included. Finally a review on mobile payment including various threats and vulnerabilities associated with such financial transactions are presented. The review of literature on mobile banking process and security aspects identifies a gap on advances in technology and actual penetration of such facilities to common mans usage. By developing better, innovative, simple, customer friendly, and more reliable online financial transaction/payment model, banks and other financial organizations can serve the customer needs in better way.

To explore the bankers perspectives to introduce mobile banking as new distribution channel and Customers perspectives on mobile banking adoption, exploratory research design is identified as appropriate. The third chapter contains an elaborative discussion on responsibility of banks while deploying online banking as new distribution channel through our new “modified customer equity approach model”. In order to explain the customer behavior of adapting mobile banking channel, we have proposed a new model called “Technology Acceptance based on Theory of Customer Stimulation by Education and Training for usage (TCSET). The new model is based on four constructs – perceived usefulness, perceived assurance, perceived ease of use, and perceived cost. These constructs stimulates the customers intention and behavior control to use mobile banking services. The various issues under, customer behavior and intention to use mobile banking transactions, like attitude, trust, convenience, perception, loyalty, privacy, security and comfort issues are discussed based on the developed model.

In third chapter, we also investigated the security threats in mobile banking implementations using the GSM network. The objective of this project is to build applications for portable devices that ensure users can securely send their banking information via the GSM network. The mobile banking solutions developed provide platforms for users to bank using SMS and GPRS. In order to enhance the security, biometric finger print detection can be used in mobile device.

In the fourth chapter, the business implications of benefits of adoption of mobile banking as a new distribution channel by Banks, business perspective of mobile banking by means of SWOT analysis, and various benefits of mobile banking from customer’s point of view are discussed. Various mobile banking models and securities in financial transactions are discussed based on the basis of variations in dimensions, and technological knowledge. In order to provide better security for financial transactions, a new mobile banking payment model called “Consumer oriented mobile business model" is proposed and discussed. The consumer oriented model allows customers to pay online for their shopping from their bank account using mobile devices. The business implications & advantages of "consumer oriented mobile business model" to decrease the possible frauds are also discussed and demonstrated for secured financial payment for online purchase. The secure SMS solution and the secure GPRS solution for the new model is also proposed which include secure SMS protocol and secure GPRS protocol. The security aspects of these solutions for the new model in terms of *Confidentiality, Integrity, Authentication, and Availability* are also discussed. To enhance the security for financial transaction a biometric authentication system is proposed. Use of this approach for mobile banking would work something like this : When a customer initiated a mobile banking transaction, the handset would request that the user register his or her fingerprint on the sensor, and the handset would compare the fingerprint to the one already stored in the phone (and, as a backup, also stored on the bank mobile transaction server). The handset would then send the transaction request and the result of the fingerprint comparison—in effect, a biometric ID authentication—to the bank server for approval and execution of the transaction. That would replace the device-based security safeguard (the SIM card) with something much more robust and harder to defeat.

5.3. Recommendation to the Customers :

Customers should make use of the new ubiquitous mobile banking distribution channel by knowing the advantages of such services. Customers should ignore fear on security of their banking account and fraudulent transactions. Customers should educate themselves to maintain the secrecy of their passwords and pin numbers to maintain secured mobile banking usage in addition to use bio-metric authentication. The following are some recommendations to the customers based on present study :

Usage of Technology :

☛ Identify the communication technology and the device technology to be used/required for optimum financial information transformation with your bank.

☛ Study the online transaction instructions from the website/brochure of the bank to avoid confusion while performing on-move transactions.

☛ Identify additional technological requirement/up-gradation to enhance security & user authentication by choosing mobile device which has bio-metric authentication facility.

Know your banks Services :

☛ Identify the various services available and their advantages/limitations from the bank personnel.

☛ Pursue the bank personnel to give training for how to use various mobile banking services using your mobile phone.

☛ Identify the service charge and incentives offered by the banks for usage of various services through your mobile device.

☛ If your bank is not providing advanced mobile banking services like utility bill payment, micro payment for retailing at shops, find out from when it will be provided.

☛ Identify the bundled services provided by the bank through mobile banking as new distribution channel.

Know your banks & mobile service providers security :

☛ Security is an important aspect of online mobile banking transactions and the usage of this channel depends on how secured the transactions are with that particular bank. The usage of mobile banking services by the customers depends on how best security is provided by the banks and the network service providers.

☛ Customers have to opt for maximum security for their transactions by means of multiple level passwords/PIN and/or voice based or bio-metric based security levels. This provides fraud less transactions of their financial information.

☛ Customers should identify the technology used by both the banks and the mobile network service providers and compare it with National leaders in the industry. If the security part of the technology is convinced, then only the customers should try for mobile banking business.

Maintenance of better security :

☛ By keeping both mobile device and the password/PIN secretly, and using the services of private network providers, the customers can avoid any fraudulent transactions from their banking account.

☛ Using 3G technology enabled mobile devices, using network of such high tech service providers, and choosing the high secured server adopted banks, customers can get better security for long term without any risk.

Better models :

☛ The new models of online banking and payment with proper research and development on improving security will certainly improve customer’s confidence on adoption of this new distribution channel.

☛ Financial payment both micro and macro level using mobile device will simplify and integrate the communication, entertainment and financial transactions so that customers can eliminate credit/debit cards.

☛ Ubiquitous financial payment through bank using mobile device allows customers to make efficient and timely decision on their investment and payments.

Confident in online services :

☛ Based on Govt. regulations and service providers' continuous technology up gradation, customers are getting confidence in online financial transaction using private networked mobile devices. Such success factors certainly improve the confidence in new users to use this new distribution channel.

☛ Since online financial services available 24 hours/365 days, and providing better convenience for customers to carryout their financial transactions, customers can enjoy the benefits of online services.

☛ By means of getting proper education and training on awareness & usage of mobile financial services available by the banks, users can definitely improve their confidence on such services.

Encash advantages :

☛ The customers should encash the advantages of mobile financial services such as anytime, anywhere, any amount of time, low cost, and moderately secured.

☛ The customers can encash the opportunity of doing cashless business/purchases/transactions using mobile device.

☛ The advantages like ubiquity, personalization, reduced cost, flexibility, increased comfort, time saving, convenience, and better cash management opportunity makes the mobile banking service as a killer application.

5. 4. General Conclusion

As the brand new banking distribution channels to Indian consumers, online and mobile banking are still at early stages in India. The current target market for online and mobile banking is relatively small due to its low level of awareness nevertheless, this should not be underestimated. There is good potential for introducing mobile banking services since, mobile banking adoption is not far behind.

In the study, it is found that the proper education and training on usage (awareness) of mobile banking services has substantial effect on attracting more customers to use this new distribution channel. With the objectives : to analyze the significance of mobile business activity in terms of their usability, opportunities, and challenges in financial sector with special emphasis on banking activities, to identify the gap between mobile communication technology innovations, their penetration in banking industry as a new distribution channel and the customer acceptance of this new distribution channel, to study present m-business models and their limitations, to propose new business model in order to accelerate the financial transaction process and to provide Value added

Services to the customers, and to provide suitable security & authentication methods to strengthen the mobile business framework in the country, the research work come to following conclusion :

1. Penetration of mobile phone usage in India : The accelerated growth of mobile phone usage in India during the last ten years and the expected reach to 600 millions by the year 2012 promises the possibility of customer acceptance of mobile banking service in near future.

2. Improved mobile banking facilities in India : Due to availability of improved technology and increased high quality mobile service providers, banks are trying to provide basic and transactional and advanced mobile banking services.

3. Understanding of various mobile communication technology and their penetration in banking sector : An overview of past, present, and future mobile banking technologies is presented. This includes review on mobile communication technology, wireless operating systems, alternative and complementary technologies, information exchange technology, location identification technology, and security considerations. An overview of wireless data services, and mobile communication devices is elaborated.

4. Bankers perspective on providing mobile banking as new distribution channel through our new “modified customer equity approach model”.

5. Customers perspective on mobile banking usage : The security and incentives by the banks have also significant affect on acceptance & usage of banking services over mobile phone. Security factor is found the most important attribute that could motivate consumers’ attitudes towards online banking in India. The present study also reveals that proper education and training (awareness) on availability and usage of mobile banking services channel is required in India to attract more customers towards usage of this new channel for their financial transactions along with other factors like technology experience, security & trust, psychology & culture, prior personal banking experience, and incentives from banks, studies in the model. Advertising messages could emphasize security for online banking and novelty for mobile banking.

6. Various m-business models and their limitations : The study also points out the requirement of new, comprehensive mobile business model for secured payment from the customers bank accounts.

7. New business model in order to accelerate the financial transaction process and to provide Value added Services to the customers : The consumer oriented model allows customers to pay online for their shopping from their bank account using mobile devices.   A brief survey on security issues in

mobile banking scenario is also discussed along with possible frauds and causes of the frauds. To enhance the security for financial transaction a biometric authentication system is proposed.

8. Finally recommendations have been made to the customers to use mobile banking services.

The study comes to the conclusion that Mobile Banking, as an interesting application in Mobile business, is winning the acceptance of the customers and enjoys sufficient demand in future days. Banks are seeing themselves increasingly forced to include Mobile Banking in their product portfolios to avoid negative differentiation against their competitors. Apart from this strategic relevance, there are other financial incentives, too. Their actual scope however depends, amongst others, on the product portfolio and the customer structure of individual banks. The study also reveal that proper education and training should be provided on availability and usage of mobile banking services to the Customers by the banks in terms of its importance, convenience, security and negligible cost.

The two security issues are addressed. A first security issue consists of the establishment of a secure channel to provide data confidentiality and data integrity of communications between a client and an authenticated bank. The second security issue is the authentication of the client, at the beginning of a session, i.e., entity authentication, and for each transaction, i.e., transaction authentication. Security is all about risks and associated costs. In a typical mobile banking system, the cost of security measures at the client side is reduced as much as possible, while keeping a minimal level of protection. One cannot achieve perfect security, so at some moment in time, despite all security measures something will always go wrong. The real question is what will happen in that case. Banks of course will want to pass liability to their users and vice versa. Law and small print on contracts will somehow make clear who will have to take the risk in the end. GSM as a stand alone medium for transporting packet data without overlying security protocols has proven vulnerable to some security attacks, with most of the authentication and confidentiality mechanisms having been cracked. This has lead to the implementation of overlying protocols such as WAP and WIG so as to enforce the security of transporting data over GSM. Most banks have taken advantage of these protocols and have implemented their mobile banking applications using the security capabilities of these protocols. Even though these protocols provide solid security for banking transactions there are some slight loopholes that could prove susceptible for mobile banking. We have provided solutions to these loopholes in two different ways; i.e. by extending and fixing problems in present bank implementations and by providing two completely new security protocols for both SMS and GPRS mediums along with bio-metric authentication process.

5.5. Limitations and Scope for Further Work

The designed protocol for secure SMS with bio-metric authentication does not necessarily limit to be use for mobile banking solution. The protocol can be altered to adapt to support secure SMS messaging solutions for peer-to-peer communication. There is no mobile application authentication in the developed J2ME application; this makes the Secure SMS/GPRS protocol susceptible to phishing. Any third party can send clients bogus mobile applications in order to acquire client sensitive information. In order to rectify this problem extra work on authentication of the mobile application is required.

The purpose of this project work is to enunciate a set of security and technology risk management guidelines for banks and payment service providers who are responsible for the design and delivery of mobile banking and payment services. It aims to provide a framework for security risk assessment and specify control and security standards applicable to the wireless environment for banking and payments.

Information security is fundamental to the reputation of the business and its underlying operations. The ability to develop and maintain market and customer confidence is contingent upon the adequacy and reliability of security practices. An attempt is made to produce a complete secure protocol for mobile banking which will cater for all network security requirements i.e. authentication, non repudiation, authorization, availability, integrity, confidentiality, and access control compared to existing mobile banking protocols.

The above work can be extended further by developing further security for transaction authentication by avoiding frauds/taping of information in the service network.

Bibliography

[1] Stallings, W. *Network Security Essentials Applications and Standards, international second ed*. Prentice Hall, 2003.

[2] Singh, G.(2002), “Securing the Mobile E-Conomy”, Retrieved from the World Wide Web: http:// www.allnetdevices.com/wireless/opinions/2002/09/11/html. 2002

[3] Porter, M. E. (1998). The Competitive Advantage of Nations (2^{nd} ed.). Basingstoke: Macmillan Business. 1998

[4] Durlacher Research Ltd. (2000), Mobile Commerce Report, February 2000. Available at http://www.sciencedirect.com /science?_ob=RedirectURL&_method= externObjLink&_locator=url&_cdi=6234&_plusSign=%2B&_target URL=www.durlacher.com (2000).

[5] Wesel, E. K.(1998), Wireless Multimedia Communications, Networking Video, Voice and Data, Addison-Wesley, Reading, MA, 1998.

[6] Veijalainen, J (1990), Transaction concepts in autonomous database environments, Ph.D. thesis, GMD-Bericht Nr. 183, R. Oldenbourg Verlag, Munich, Germany, April 1990, ISBN 3-486-21596-5.

[7] Barnett, N., Hodges, S., & Wilshire, M. J. (2000). M-Commerce: An Operator's Manual. McKinsey Quarterly, 3, p-162-173. Retrieved from the World Wide Web: http://www.libfind.unl.edu:2020/journals/iris/busis.html., 2000

[8] Clarke, I. (2001) Emerging value propositions for m-commerce. Journal of Business Strategies, **18**, pp. 133–148, 2001

[9] Muller-Veerse, F. (2000), Mobile business Report, 2000, Durlacher Corporation, Retrieved from the World Wide Web: http://www.durlacher.com/downloads/mcomreport., 2000

[10] Keng Siau (2001), “Mobile Commerce : Promises, Challenges and Research Agenda” J. of Database Management, Vol 12, 3, 2001, pp. 4-14, 2001

[11] Varshney, U., & Vetter R. (2001), “A Framework for the Emerging Mobile business Applications”. Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.

[12] Deitel, H.M., Deitel, P.J., & Steinbuhler, K. (2001), e-Business and e-business for Managers, Upper Saddle River, New Jersey: Prentice Hall 2001.

[13] WAP Forum, *Wireless Application Protocol Architecture Specification*, Version 12-Jul-2001, available from http://www.wapforum.org, 2001.

[14] Lam, K.Y, Cung, S., Gu, M., and Sun, J., *Lightweight Security for Mobile Commerce Transactions*. Computer Communications 26, 2052 -2060, 2003

[15] Web Pro Forums (2007), *Wireless Short Message Service (SMS)* available at International Engineering Consortium: http://www.iec.org/, 2007

[16] Steve Lord (2003), *Trouble at the Telco: When GSM Goes Bad Network Security*, (1), p 10-12, 2003

[17] Niina Mallat, Matti Rossi, and Virpi Kristiina Tuunainen, *Mobile Banking Services Communications of the ACM,* 47, 5 pp 42-46, 2004

[18] Arumuga perumal S., (2006), Effective Method of Security Measures in Virtual Banking, Journal of Internet Banking and Commerce, April, vol. 11, no.1, 2006

[19] MacGregor, R., Ezvan, C, and Liquori, L., (1997), Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice. SG24- 4978-00 Redbook, IBM, International Technical Support Organization, Raleigh, NC, July 2, 1997; see www.redbooks.ibm.com/., 1997

[20] Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication FIPS 186. U.S. Department of Commerce, Washington, DC, May 1994.

[21] Ratshinanga, H., Lo, J., Bishop, *A Security Mechanism for Secure SMS Communication. Department of Computer Science, University of Pretoria, South Africa.* (Online) http://polelo.cs.up.ac.za/papers/SecureSMS.pdf. 2004

[22] Herzberg, A. 2003. Payments and banking with mobile personal devices. *Communications of the ACM* .Volume 46, Issue 5, Wireless networking security Pages: 53 58 ISSN: 0001-0782, May 2003

[23] M. Slemko, "Microsoft passport to trouble", http://alive.znep.com/~marcs/passport/UTH, 2003.

[24] T. Dierks and C. Allen, "The TLS Protocol Version 1.0. IETF Request for Comments", RFC 2246, January 1999.

[25] Wireless Application Protocol Forum, "WAP Wireless Transport Layer Security", Version 06, April 2001.

[26] E. Rescorla, "SSL and TLS: Designing and Building Secure Systems", Addison-Wesley, 2000.

[27] J. Soroor, "Models for Financial Services Firms in Developing Countries Based upon Mobile Commerce", International Journal of Electronic Finance, Inderscience Publishers, 2006.

[28] H. Dobbertin, "The Status of MD5 After a Recent Attack", RSA Laboratoriesâ€™ CryptoBytes 2(2), pp. 1-6, 1996.

[29] R. Morris and K. Thompson, "Password Security: A Case History", Communications of the ACM, 22(11), pp. 594-597, 1979.

[30] N. Haller, C. Metz, P. Nesser, and M. Straw, "A One-Time Password System", IETF Request for Comments, RFC 2289, 1998.

[31] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, 24(11), pp. 770-772, November 1981.

[32] A. Shamir and N. van Someren, "Playing â€œHide and Seekâ€� with Stored Keys", in: M. Franklin, editor, Proceedings of the Third International Conference on Financial Cryptography, Lecture Notes in Computer Science, LNCS 1648, Springer-Verlag, pp. 118-124, 1999.

[33] D. Janssens, R. Bjones, and J. Claessens, "KeyGrab TOO â€“ The search for keys continues...", Utimaco White Paper, http://www.utimaco.com/UTH, 2000.

[34] SecurID, http://www.rsasecurity.com/UTH.

[35] Digipass, http://www.vasco.com/UTH.

[36] M. Jakobsson and S. Wetzel, "Security Weaknesses in Bluetooth", in: D. Naccache, editor, "Topics in Cryptology â€“ Proceedings of the Cryptographersâ€™ Track at RSA 2001", Lecture Notes in Computer Science, LNCS 2020, Springer-Verlag, pp. 176-191, 2001.

[37] J. Soroor, "Models for Financial Services Firms in Developing Countries Based upon Mobile Commerce", International Journal of Electronic Finance, Inderscience Publishers, 2006.

[38] P. A. Loscocco, S. D. Smalley, P. A. Muckelbauer, and R. C. Taylor, "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments", in the Proceedings of the 21st National Information Systems Security Conference, pp. 303-314, October 1998.

[39] FINREAD, "Financial Transactional IC Card Reader", CEN Workshop Agreement, CWA 14174, 2002.

[40] TCPA, "Trusted Computing Platform Alliance", http://www.trustedpc.org/UTH.

[41] A. Spalka, A. B. Cremers, and H. Langweg, "Protecting the Creation of Digital Signatures with Trusted Computing Platform Technology Against Attacks by Trojan Horse Programs", in: M. Dupuy and P. Paradinas, editors, "Trusted Information â€“ The New Decade Challenge", Proceedings of IFIP SEC 2001, Kluwer Academic Publishers, pp. 403-419, 2001.

[42] S. Garfinkel and G. Spafford, "Practical UNIX & Internet Security", 2nd Edition, O’Reilly, 1996.

[43] Javad Soroor, Implementation of a Secure Internet/Mobile Banking System in Iran Journal of Internet Banking and Commerce, December 2005, vol. 10, no.3 (http://www.arraydev.com/commerce/jibc/), 2005

[44] The Boston Consulting Group(2000). Mobile Commerce: Winning the On-Air Consumer Report, Nov. 2000. Theory and Application, 3(4), 2000

[45] Autio, E, Bout D, Golub G, Hayrinen J, Kohlenbach B, Laitinen S, Muller-Veerse F, and Singh S. (2001), UMTS Report—An Investment Perspective. Durlacher Research Ltd, London, Eqvitec Partners, Helsinki, Helsinki University of Technology, Helsinki, Mar. 2001.

[46] Rasanen J. (2001) From messaging to 3G: Enabling the mobile access. Presentation at CeBIT 2001. FirstHop, Mar. 2001.

[47] Lin Y. B., and I. Chlamtac (2001). Wireless and Mobile Network Architectures. JohnWiley & Sons, New York, NY, USA, 2001.

[48] Daniel, E.M. and H.M. Wilson, (2003), "The Role of Dynamic Capabilities in E-Business Transformation," European Journal of Information Systems, Vol. 12, pp. 282-296, 2003

[49] Utterback J. M., (1994), Mastering the Dynamics of Innovation, Harvard Business School Press, Boston, MA, 1994

[50] Christensen C. M., (1997), The Innovator’s Dilemma, Harvard Business School Press, Boston, Massachusetts, 1997.

[51] Du Preez G. T., C.W.I. Pistorius C.W.I., (2002) Analyzing technological threats and opportunities in wireless data services, Technological Forecasting & Social Change 70, pp. 1–20, 2002

[52] Dalglish, B., (1999), Telecom technology for non-techies: a refresher on some basics of telecommunications technology. TelecomTechStocks. Com, 1999

[53] Standard & Poor’s Industry Surveys, 2002. Communications Equipment, Current Environment, January 31, 2002

[54] Palm, Inc. Website, 2002. http://www.palm.com

[55] Karnouskos, S. and Fraunhofer, F. (2004) ‘Mobile payment a journey through existing procedures and standardization initiatives’, IEEE Communications Surveys, Vol. 6, No. 4, pp.44–66, 2004

[56] McMahon, R.A., DeVries, P.D. and Chong, P.P. (2005) ‘Building a wireless network infrastructure under budget constraints’, International Journal of Mobile Communications, Vol. 3, No. 4, pp.445–456, 2005

[57] Walker, B. and Barnes, S.J. (2005), ‘Wireless sales force automation: concept and cases’, International Journal of Mobile Communications, Vol. 3, No. 4, pp. 411–427, 2005

[58] Chameleon Network (2003) ‘Pocket vault frequently asked questions’, 14 April, Available at: http://www.chameleonnetwork.com/faq.htm, 2003

[59] Young B. Choi, Rachel L. Crowgey and James M. Price, Joseph S. VanPelt, (2006), The state-of-the-art of mobile payment architecture and emerging issues Int. J. Electronic Finance, Vol. 1, No. 1, pp. 94 – 103, 2006

[60] Herzberg, A. (2003), Payments and banking with mobile personal devices, Communications of the ACM, Vol. 46, No. 5, pp. 53-58, 2003

[61] Sathye, M. (1997), Internet Banking In Australia, Journal of Internet Banking and Commerce, Vol.2, No. 4, September 1997.

[62] Booz-Allen & Hamilton, Inc. (1997)."Booz-Allen's Worldwide Survey Revealed A Huge Perception Gap Between Japanese And American/European Banks Regarding Internet Banking." 1997

[63] Egland, Kori L., Karen Furst, Daniel E. Nolle, Douglas Robertson (1998). Banking over the Internet, Quarterly Journal, Vol. 17, No. 4, Office of Comptroller of the Currency, December, 1998

[64] Furst K, Lang W. W. and Nolle E. Daniel (1998), Technological Innovation in Banking and Payments: Industry Trends and Implications for Banks, Office of the Comptroller of the Currency, Quarterly Journal, Vol. 17, No. 3, September, 1998

[65] Diniz, Eduardo (1998), “Web banking in USA” Journal of Internet Banking and Commerce, Vol.3, No.2, June, 1998

[66] Furst, K., Lang, W. W., & Nolle, D. E. (2000). Internet banking: Developments and prospects (Economic and Policy Analysis Working Paper 2000-9). Washington: Office of the Comptroller and Currency, 2000

[67] Sullivan, R.J. (2000), How Has the Adoption of Internet Banking Affected Performance and Risk at Banks? A Look at Internet Banking in the Tenth Federal Reserve District, Financial Industry Perspectives, Federal Reserve Bank of Kansas City, December, 2000

[68] Guru, B., Vaithilingam, S., Ismail, N. and Prasad, R. (2000). Electronic Banking in Malaysia: A Note on Evolution of Services and Consumer Reactions. Journal of Internet Banking and Commerce, Volume 5, No. 1, June, 2000

[69] DeYoung, R (2001a), Learning-by-Doing, Scale Efficiencies, and Financial Performance at Internet-Only Banks, Working Paper 2001-06, Federal Reserve Bank of Chicago, September, 2001

[70] DeYoung, R (2001b), The Financial Performance of Pure Play Internet Banks, Economic Perspectives 25(1): 60-75, Federal Reserve Bank of Chicago, 2001

[71] Jasimuddin, Sajjad M. (2001), “Saudi Arabian Banks on the Web” Journal of Internet Banking and Commerce, Vol.6, No.1, May, 2001

[72] Ndubisi, N.O. and Jantan, M. (2003), ‘‘Evaluating IS usage in Malaysian small and medium-sized firms using the technology acceptance model’’, Logistics Information Management, Vol. 16 No. 6, pp. 440-50, 2003

[73] Furst, K; Lang, W., William and Nolle, E., Daniel (2002). Internet Banking: Developments and Prospects, Working Paper, Center for Information Policy Research, Harvard University, April, 2002

[74] Koedrabruen, P. and Raviwongse R. (2002), A Prototype of a Retail Internet Banking for Thai Customers, Scuola Superiore Guglielmo Reiss Romoli (SSGRR), May 31, 2002

[75] Corrocher, N. (2002), Does Internet banking substitute traditional banking? Empirical evidence from Italy, Working Paper, CESPRI, No. 134, November, 2002

[76] Hasan, I., (2002). Do Internet Activities Add Value? The Italian Bank Experience, Working Paper, Federal Reserve Bank of Atlanta, New York University, 2002

[77] Janice, David and Dennis (2002), Click and Mortar of Retail Banking A Case Study in Hong Kong, Nanyang Business School, Nanyang Technological University, 2002

[78] Lustsik, O.(2003), E-Banking in Estonia: Reasons and Benefits of Rapid Growth, Kroon & Economy, No. 3, 2003

[79] Awamleh R, Evans J and Mahate A. (2003), Internet Banking in Emerging Markets The Case of Jordon **-** A Note, Journal of Internet Banking and Commerce, Vol. 8, No. 1, June, 2003

[80] Mari Suoranta, and Minna Mattila, (2003) Mobile banking and consumer behaviour: New insights into the diffusion pattern, Journal of Financial Services Marketing Vol. 8, 4, pp. 354–366, 2003

[81] Jukka Riivari, (2005) Mobile banking: A powerful new marketing and CRM tool for financial services companies all over Europe, Journal of Financial Services Marketing, Vol. 10, 1 pp. 11–20, 2005

[82] Mari Suoranta, Mattila, M. and Munnukka, J. (2005) ‘Technology-based services: a study on the drivers and inhibitors of mobile banking’, Int. J. Management and Decision Making, Vol. 6, No. 1, pp. 33–46, 2005

[83] Irwin Brown, and Alemayehu Molla, (2005**),** Determinants of Internet and Cell Phone Banking Adoption in South Africa, Journal of Internet Banking and Commerce JIBC, Vol. 10, 1, 2005

[84] Vijayan P, Vignesen Perumal, Bala Shanmugam, (2005), Multimedia Banking and Technology Acceptance Theories in Malysia, Journal of Internet Banking and Commerce JIBC, Vol. 10, 1, 2005

[85] Unnithan, C. R. and Swatman, P. (2001), Ebanking Adaptation and Dot.Com Viability Comparison of Australian and Indian Experiences in the Banking Sector, Working Paper, School of Management Information Systems, Deakin University, No. 14, 2001

[86] Rao, G. R. and Prathima, K. (2003), Internet Banking in India, Mondaq Business Briefing, April 11, 2003

[87] Agarwal, N., Agarwal, R., Sharma, P. and Sherry, A. M. (2003), Ebanking for comprehensive EDemocracy: An Indian Discernment, Journal of Internet Banking and Commerce, Vol. 8, No. 1, June, 2003

[88] Balwinder Singh, and Pooja Malhotra,(2004) Adoption of Internet Banking: An Empirical Investigation of Indian Banking Sector, Journal of Internet Banking and Commerce, July 2004, vol. 9, no. 2., 2004

[89] Sakkthivel, A. M., (2006), Impact of Demographics on the Consumption of Different Services Online in India, Journal of Internet Banking and Commerce, December 2006, vol. 11, no. 3, 2006

[90] Mookerji, N. (1998), Internet Banking Still in Evolutionary Stage, at www.financialexpress.com/fe/daily/19980714/19555264.html, July 14, accessed as on August 22, 2003.

[91] Pegu, R. (2000), Net-Banking is Fast Becoming Popular, The Week, June 25, 2000.

[92] Dasgupta, P. (2002), Future of E banking in India, available at www.projectshub.com December, accessed as on August 16, 2003.

[93] Jain, S. (2006, October). “A Mobile Security Battle.” Security, 43(10), 66-67, 2006

[94] Tang, J., Terziyan, V., Veijalainen, J. (2003), “Distributed PIN Verification Scheme for Improving Security of Mobile Devices.” Mobile Networks and Applications, 8(2), 159, 2003

[95] Clarke, N. L., & Furnell, S. M. (2005). “Authentication of users on mobile telephones -- A survey of attitudes and practices.” Computers & Security, 24(7), 519-527, 2005

[96] Mazhelis, O., & Puuronen, S. (2007). “A framework for behavior-based detection of user substitution in a mobile context.” Computers & Security, 26(2), 154, 2007

[97] Feig, N. (2007, November). “Authentication Goes Mobile -- Banks look to out-of band authentication as customers seek enhanced online banking security.” Bank Systems & Technology, 44(11), 23, 2007

[98] ClairMail Security White Paper. (2007, July). Retrieved February 2008. Available:
http://www.pdfdownload.org/pdf2html/pdf2html.php?url=http%3A%2F%2Fwww.
ClairMail.com%2Fproducts%2F..%2Fdownloads%2FClairMail_Security_White_Paper.pdf&images=yes

[99] Clarke, N. L., & Furnell, S. M. (2007b). “Authenticating mobile phone users using keystroke analysis.” International Journal of Information Security, 6(1), 1, 2007

[100] Lin, P. P., & Brown, K. F. (2007). “Smartphones Provide New Capabilities for Mobile Professionals.” The CPA Journal, 77(5), 66-71, 2007

[101] MacLeod, M. (2006, December). “Success of mobile devices builds security opportunities.” MicroScope, 16, 2006

[102] Miller, C. (2007, August). “ISE Hacks to Protect iPhone.” Design News, 62(11), 18, 2007

[103] Goodwin, B. (2005, September). “PDAs and mobiles left open to 'Bluesnarfing'.” Computer Weekly, 8, 2005

[104] Vandini, C. (2008). “Cell phone cloning stuns owners: Unsuspecting victims surprised by high bills, extra calls.” McClatchy - Tribune Business News, 10, March 2008

[105] Yuh-Min Tseng (2007). “A secure authenticated group key agreement protocol for resource-limited mobile devices.” The Computer Journal, 50(1), 41-52, 2007

[106] Berger, B. (2007, March). “Protecting Enterprise Data on Mobile Systems with Trusted Computing.” Security, 44(3), pp 70,72,74, 2007

[107] Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M. Gómez-Skarmeta. A. F. (2007). "A Survey of Electronic Signature Solutions in Mobile Devices." Journal of Theoretical and Applied Electronic Commerce Research, 2(3), 94-109, 2007

[108] Malykhina, E. (2006, November), "Smartphones Under Fire." InformationWeek, (1114), 55-56, 2006

[109] Conry-Murray, A. (2005, December). "Mobile Anti-Virus: Now or Later?" IT Architect, 20(12), 92-95, 2005

[110] Saran, C. (2005, October). "Nokia counters malware threat to data on its smartphones." Computer Weekly, 26, 2005

[111] Schneider, G. (2007). Electronic Commerce Security. In Electronic Commerce (Seventh Annual Edition ed.). (PP. 438-483) Boston, Massachusetts, United States of America: Thompson Learning Inc, 2007

[112] ePayNews.com (2002) 'ePayNews.com Statistics' 2002, at http://www.epaynews.com/statistics/mcommstats.html#47

[113] Atos (2005) 'Telecoms Predictions 2006', Atos Consulting, at http://www.atosorigin.com/NR/rdonlyres/3AEB9CEF-FB75-4259-9D72-92C66331C7D9/0/rp_Atos_Origin_Predictions.pdf+M-Commerce+growth+predictions+2006&hl=en&ct=clnk&cd=9&client=safari

[114] Moses A. (2008) 'Mobile banking steps up a gear' The Melbourne Age, 31 January 2008, at http://www.theage.com.au/articles/2008/01/31/1201714114004.html

[115] Pousttchi K. (2003) 'Conditions for Acceptance and Usage of Mobile Payment Procedures' In Giaglis G.M., Werthner H., Tschammer V. & Foeschl K. (Eds.) 'mBusiness 2003 - The Second International Conference on Mobile Business' Vienna, 2003 (pp. 201-210), at http://www.wi-mobile.org/fileadmin/Papers/MP/Conditions-for-acceptance-and-usage-of-mobile-payment-procedures_10-07.pdf, 2003

[116] MPF (2006) 'Mobile Proximity Payment Issues and Recommendations: Mobile Payment Configuration and Maintenance' Mobile Payment Forum, v.1.0, October 2006, at http://www.mobilepaymentforum.org/documents/Proximity_Payment_IR_11_0.pdf, 2006

[117] Scornavacca E.,Barnes S.J. & Huff S.L. (2005) 'Mobile Business Research, 2000-2004: Emergence, Current Status, And Future Opportunities' Proc. Euro. Conf. on Information Systems, 2005

[118] Scornavacca E. (2007) 'M-Lit Search' Victoria University of Wellington, at http://www.m-lit.org/

[119] Linck K., Pousttchi K. & Wiedemann D. G. (2006) 'Security issues in mobile payment from the customer viewpoint' Proc. 14th Euro. Conf. on Information Systems (ECIS), 2006

[120] Dahlberg T., Mallata N., Ondrusb J. & Zmijewska A. (2007) 'Past, present and future of mobile payments research: A literature review' Working Paper, February 2007

[121] Lee C., Kou W. & Hu W.C. (Eds.) (2004) 'Advances in Security and Payment Methods for Mobile Commerce' IGI Global, 2004

[122] Choi Y.B., Crowgey R.L., Price J.M. & VanPelt J.S. (2006) 'The state-of-the-art of mobile payment architecture and emerging issues'Int. J. of Electronic Finance 1, 1 (2006) 94 – 103, 2006

[123] Rawson S. (2002) 'E-commerce mobile transactions: Mobility and liability: The hazards of handhelds' Computer Law & Security Report 18, 3 (2002) 164-172, 2002

[124] Kreyer N., Pousttchi K. & Turowski K. (2003) 'Mobile Payment Procedures: Scope and Characteristics' e-Service Journal 2, 3, 7-22, 2003

[125] Zmijewska A. (2005) 'Evaluating Wireless Technologies in Mobile Payments - A Customer Centric Approach' Proc. International Conference on Mobile Business (ICMB'05), pp. 354-362, 2005

[126] van der Heijden H. (2002) 'Factors Affecting the Successful Introduction of Mobile Payment Systems' Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 17 - 19, 2002

[127] Misra S.K. & Wickramasinghe N. (2004) 'Security of a mobile transaction: A trust model' Electronic Commerce Research 4, 4 (October 2004) 359-372, 2004

[128] Clarke R. (1996b) 'The SET Approach to Net-Based Payments' Xamax Consultancy Pty Ltd, November 1996, at http://www.rogerclarke.com/EC/SETOview.html

[129] Visa (2008) 'Visa Authenticated Payment Program', February 2008, at https://partnernetwork.visa.com:443/vpn/global/category.do?userRegion=1&categoryId=85&documentId=117

[130] Roger Clarke, 2008 A Risk Assessment Framework for Mobile Payments, Proc. 21st_Bled e-Commerce Conf., June 2008, pp. 63-77, 2008, http://www.rogerclarke.com/EC/MP-RAF.html,

[131] Mols, N.P., Bukh, P.N.D. and Nielsen, J.F. (1999), Distribution Channel strategies in Danish retail Banking”, International Journal of Retail & Distribution Management, Vol. 27 No. 1, pp. 37-47, 1999

[132] Mahajan, V., Muller, E. and Bass F., (1990), 'New Product Diffusion Models in Marketing, a Review and Directions for Research', Journal of Marketing, 54, pp. 1-26, 1990

[133] Rogers, E.M., (1995), ' Diffusion of Innovation', The Free Press, NY., 1995

[134] Ajzen, I. and Fishbein, M. (1980), 'Understanding attitudes and predicting social change', Prentice-Hall, Englewood Cliffs, NJ., 1980

[135] Fishbein, M. and Ajzen, I. (1975), Belief, attitude, intention, and behavior: an introduction to theory and research, Addison-Wesley, Reading, MA. 1975

[136] Taylor, S. and P. A. Todd, (1995) “Understanding Information Technology Usage: A Test of Competing Models,” Information Systems Research, Vol. 6, No. 3, pp. 144-176., 1995

[137] Sirdeshmukh, D., Singh, J. and Sabol, B. (2002) ‘Consumer trust, value and loyalty in relational exchanges’, Journal of Marketing, Vol. 66, No. 1, pp. 15–37, 2002

[138] Walker, B. and Barnes, S.J. (2005), ‘Wireless sales force automation: concept and cases’, International Journal of Mobile Communications, Vol. 3, No. 4, pp. 411–427., 2005

[139] Bielski, L. (2003) ‘Striving to create a safe haven online’, American Bankers Association (ABA) Banking Journal, Vol. 95, No. 5., 2003

[140] Steve Lord, X-Force Security Assessment Services, and Internet: Trouble at the Telco When GSM goes bad. In *Network Security*, 2003(1):10 12, 2003

[141] Margrave, D. *GSM Security and Encryption*. Available from: http://www.hackcanada.com/blackcrawl/cell/gsm/gsmsecur/gsm-secur.html (1999); accessed 27 October 2006.

[142]. Wagner, D. *GSM Cloning*. Smartcard Developer Association and ISAAC security research group. Available from: http://www.isaac.cs.berkeley.edu/isaac/gsm.html (1998); accessed 28 October 2006.

[143] WAP Forum, Wireless Application Protocol Architecture Specification, Version 12-Jul-2001, available from http://www.wapforum.org, 2001.

[144] Burak Bayoglu: Performance evaluation of WTLS handshake protocol using RAS and elliptic curve cryptosystems, 2004.

[145] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[146] Arumuga perumal S., (2006), Effective Method of Security Measures in Virtual Banking, Journal of Internet Banking and Commerce, April 2006, vol. 11, no.1., 2006

[147] Senior, Adriana, (1999), "Branding, Money Concerns Halt a Web-Only Plan," American Banker (164), pp. 1-3., 1999

[148] Leuchter, Miriam (1999), "Which Way on the Internet ?" US Banker (109:9), pp. 36-43., 1999

[149] Peffers, K. (2001). The future of electronic commerce: A shift from the EC, The Week, May 18, 2001.

[150] Lewis, B.R., Orledge, J. and Mitchell, V. (1994), “Service quality: students’ assessment of banks and societies”, International Journal of Bank Marketing, Vol. 12 No. 4, pp. 3-12, 1994

[151] Pyun, C., Scaggs, L. and Nam, K. (2002), “Internet banking in the US, Japan, and Europe”, Multinational Business Review, Fall, pp. 73-81., 2002

[152] Hightower, J., & Borriello, G. (2001). Location systems for ubiquitous computing. IEEE Computer, 34(8), 57-66., 2001

[153] Kiesnoski, K. (2000). Wireless banking. Bank Systems and Technology, 37(2), 40-43., 2000

[154] MacGregor, R., Ezvan, C, and Liquori, L., (1997), Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice. SG24- 4978-00 Redbook, IBM, International Technical Support Organization, Raleigh, NC, July 2, 1997; see www.redbooks.ibm.com/.

[155] Horn, G. and Preneel, B. (1998), Authentication and payment in future mobile systems. In Proceedings of the European Symposium on Research in Computer Security (ESORICS’98) Lecture Notes in Computer Science (Louvainla- Neuve, Belgium, Sept. 6–8). Springer Verlag, pp. 277–293, 1998.

[156] Herzberg, A. (2003), Payments and banking with mobile personal devices, Communications of the ACM, Vol. 46, No. 5, pp. 53-58, 2003

[157] Biryukov, A. Shamir, A. Wagner, D. Real Time Cryptanalysis of A5/1 on a PC. In *Fast Software Encryption Workshop*, 2000

[158]. Horn, G. and Preneel, B., Authentication and payment in future mobile systems. In Proceedings of the European Symposium on Research in Computer Security (ESORICS’98) Lecture Notes in Computer Science (Louvainla- Neuve, Belgium, Sept. 6–8). Springer Verlag, pp. 277–293, 1998

[159] Joseph Tan, H. Joseph Wen, Tibor Gyires, M-commerce security: the impact of wireless application protocol (WAP) security services on e-business and e-health solutions, International Journal of Mobile Communications, Volume 1, Number 4, pp 409 – 424, 2003

[160] Stallings, W. *Network Security Essentials Applications and Standards, international second ed.* Prentice Hall, 2003.

List of Publications

1. “Promises, Challenges, and Research Opportunities for Mobile Business Activity in India” is presented at National Conference on Infrastructure Management : Emerging Issues, Manipal Institute of Management, Manipal, 16 – 18 May 2003.

2. “Challenges in Emerging Mobile Business Services in India” published in Proceedings of two days workshop on Emerging Management Issues in Service Industry - Manegma 2004, Vol. 2, Page 41 – 49, held at Srinivas Institute of Management Studies, Mangalore.

3. Mobile Device based E-learning Model : a Classical Solution for Global Reach P. S. Aithal, and Santhosh Prabhu ; International conference on “Reshaping Management Education in Global Context” on 15 – 16 November 2003, Institute of Management Studies, Devi Ahilya University, Indore, India.

4. Marketing online banking services using Mobile Devices : An Indian prospective, Presented in International Conference on Services Management at New Delhi, March 11-12, 2005.

5. Benefits, Challenges and Prospects of Online Retail Banking in India. Presented at National Conference on Management of “Emerging Sectors” : New Paradigms and perspectives, held at Bapuji Institute of Management Studies, Davangere, India, during 15 & 16 April, 2005.

6. Mobile Banking Initiatives and Models in Indian Private & Public Sector Banks Presented for Strategy Summit 2005 – Living the future, ICFAI Business School, Calcutta. 15-16, February 2005.

7. Security Issues in Online Financial Transactions with Special Reference to Banking & Insurance Industry, Presented at National Conference on Quality in Service Sector and Managerial Challenges, Manipal Institute of Management, Manipal, 21-22, May 2005.

8. Ubiquitous Banking : Exploiting Information Technology for Financial Transactions in Banking Industry, Presented at International Conference on Exploiting Information Science, Systems & Technology for Organizational Enhancement MDI, New Delhi, July 24-26, 2005, Delhi, India.

9. Security Issues in Online Financial Transactions with Special Reference to Banking Industry, by P.S. Aithal**,** Srinivas Institute of Management Studies, Mangalore, India – 575 001 & K.V.M. Varambally**,** Manipal Institute of Management, Manipal, India – 576 119 published in Quality in Service Sector and Managerial Challenges – Allied Publisher Pvt. Ltd. 2006, Page 103- 114.

10. Wireless Communication in Service Sector – Issues & Challenges, P.S. Aithal, Srinivas Institute of Management Studies, Mangalore 575 001, published in Proceedings of National Workshop on Strategic Re-thinking – Contemporary Issues, Manegma 2007, held at Srinivas Institute of Management Studies, on 24th March 2007.

11. Marketing Online Banking Services Using Mobile Devices : An Indian Prospective, by P.S. Aithal, Srinivas Institute of Management Studies, Mangalore, India – 575 001 & K.V.M. Varambally, Manipal Institute of Management, Manipal, India – 576 119, accepted for publication in Journal of Internet Banking and Commerce, (http://www.arraydev.com/commerce/jibc/)

12. Presented research paper titled “Mobile Business in Developing World: An Innovative Technology based competitiveness in Productivity enhanced Business Transaction” Dr. P.S. Aithal, at European Productivity Conference (EPC) 2009 held during 28-30th October 2009 at Grimsby, U.K.

13. Technological Management and Mobile Business Services in India – A Futuristic Approach by P.S. Aithal, Srinivas Institute of Management Studies, Mangalore, India – 575 001 & K.V.M. Varambally, Manipal Institute of Management, Manipal, India – 576 119, Published in Proceedings of International Conference in 10th South Asian Management Forum 2009 on “Change and Continuity : Management Prospects and Challenges” during 9-10th April 2009, Organized by Royal Institute of Management, Bhutan. Page : 121 -139, 2009

14. Mobile Business Technology and Business Proliferation of Banks – A futuristic Approach by P.S. Aithal, & K.V.M. Varambally, Amity Business Review – an Indian Journal, Vol. 10 , No. 1, pp 9-25, 2009