A Study on Multi Phase Security Solutions to ATM Banking Systems

Krishna Prasad K.
College of Computer and Information Sciences,
Srinivas University, Pandeshwar, Mangalore-57501, India
Email:karanikrishna@gmail.com

Type of the Paper: Research Paper.
Type of Review: Peer Reviewed.
Indexed In: OpenAIRE.
Google Scholar Citation: IJAEML

How to Cite this Paper:
Krishna Prasad, K. (2018). A Study on Multi Phase Security Solutions to ATM Banking Systems. *International Journal of Applied Engineering and Management Letters (IJAEML), 2*(2), 116-126.

International Journal of Applied Engineering and Management Letters (IJAEML)
A Refereed International Journal of Srinivas University, India.

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

A Study on Multi Phase Security Solutions to ATM Banking Systems

Krishna Prasad K.
College of Computer and Information Sciences,
Srinivas University, Pandeshwar, Mangalore-57501, India
Email:karanikrishna@gmail.com

ABSTRACT

The growth in electronic transactions and banking system has resulted in greater demand for fast access of banking transactions with the aid of Automated Teller Machine (ATM). The quick increment in the utilization of ATM transactions has been closely followed by the increase in ATM frauds. The security problem and fraudulent transactions are the biggest deterrents in the continuous or widespread use of ATM transactions. For the security of ATM just possession of password or prior knowledge of computer systems or ATM machines not altogether enough. In ATM, security is essential in different aspects including physical machines, transactions, user authentication and integrity and finally user security itself. Hence fraud prevention and security has become essential ingredients in order to increase the number of ATM users and to improve client trust and confidence over ATM's. This paper explains about and examines the different types of security breaches in ATM banking systems. This paper also expounds improved security solutions to ATM's in multiphase's, which take into accounts all the aspects of security in all fields of ATM banking system, which is derived through focus group interaction. This paper could assume a functioning job in genuine research on ATM transaction framework security.

Keywords: ATM, Life Cycle Security, Integrity, Authentication.

I. INTRODUCTION :

Rapid developments of banking technology changed the managing an account money exchanges with the chance to go for able, quick, adaptable and practical model. One banking technology innovation that has diminished or totally evacuated physical communication with bank staff and affected decidedly and adversely to managing an account exercises and exchanges is the presentation of computerized teller machine (ATM) [1]. When a new technology advents the success and continuation is determined by the member of the society through the diffusion of new technological innovation.

However ATM technology has dominated and extended all over the world and bank staff and customers are relaxed more, due to exclusion they received from hassles of bank transactions, paper based validation and a long queue. With an ATM customer is able to conduct few core transactions such as cash withdrawal, cash deposit, balance enquiry, mini statement, and last few transaction details and other subsidiary transactions like paying phone and electricity bills. An ATM is moreover described with diverse names as computerized managing an account machine, money point, money machine [2-3].

The speedy expansion in the utilization of ATM exchanges has been nearly trailed by the expansion in ATM fakes. Despite the fact that individual ID number (PIN) or secret password is one vital angle in the security of ATM exchanges, numerous different kinds of securities are fundamental, for example, security of ATM machine, security of the user and safety measures of the card. With the expansion of ATM cheats new confirmation systems are produced [4].

In the present business atmosphere layered security is received with the end goal to give greater security to ATM. This layered security incorporates physical security of the machine, transaction security, client validation security, client security. To hold the current clients and to enhance their trust and trust in the security of ATM managing an account framework or automated banking systems must create distinctive refined systems to shield from illegal access to clients accounts and furthermore self security of the client. The paper is arranged as follows. Section II provides the background of ATM security and need for multiphase security (lifecycle security). Section III introduced related work on ATM security. Section IV provides new paradigm to security through security life cycle. Section V analyzes the security life cycle. Section VI concluded the paper.

2. RESEARCH BACKGROUND :

Crime at ATM has twisted away to be in general issue that influences user as well as financial institutions or bank services that makes them to be questionable about doing money exchanges over the portable/cell-phone system [5]. The distinctive sort of ATM attacks are attacks to ATM machines itself with the end goal to access money inside safe, robbery of bank card data robbery of delicate data or controlling ATM heave charges naturally and in most noticeably awful making radical harm the life of client itself. The current strategies of client verification include the ATM card with its ID number and PIN experiences a few provisos [6]. Secret password or PIN can be effectively obtained by direct covered perceptions. At the point when ATM card is stolen or lost, an unapproved or unauthorized client can without much of a stretch figure the PIN, in light of the fact that even subsequent to controlling ordinarily a few clients will utilize PIN number as their birthday date, telephone number or government managed savings numbers.

With the end goal to hold the current client trust and confidence and get new clients, financial organizations should fuse more beached safety system and there by defeat from fraudulent clients. Extortion moves in numerous ways crosswise over channel, from web to ATM machines by taking client ATM card from the confirmed/authorized client. It is extremely fundamental and important to see security from multi-phase perspective, with the end goal to screen and counter quickly moving extortion of exceedingly advanced nature. Multi-phase security includes Physical Security, ATM card Security, Transnational and Network Security, Authentication Security and User Security.

3. RELATED WORK :

Shaikh and Rabaiotti (2010) [7] reviewed and examined United Kingdom identity card and they discovered that there is an exchange off between exactness, security and adaptability in biometric based identity framework where emphasis on one undermines other. Amurthy and Redddy (2012) [8] built up an embedded unique mark framework or fingerprint system, in which client database contains client unique finger impression and cell-phone numbers alongside some fundamental data identified with records. At the point when the client puts a finger on the unique mark module it consequently creates each time unmistakable four digit code and that sent to client approved cell-phone through GSM associated with the micro-controller. Client is offered access to ATM machines in the wake of checking the code entered by the client is substantial one or not.

Onyesolu and Ezeani (2012) [9] proposed an embedded fingerprint biometric authentication scheme for Automatic Teller Machine (ATM). They surveyed customers and staff of some commercial banks in Awka, Anambra State, South-Eastern Nigeria using 16-item questionnaire consisting of participants profile, participants' use and reliability of ATM and reliability of fingerprint biometric characteristic as three sections. They found that all the customers of ATM machines aware of ATM frauds and the incorporation of finger print to the existing ATM card and PIN will provide a better security to the ATM. Subha and Vanithaasri (2012) [10] proposed a multimodal biometric data framework to give shared authentication and key generation in the ATM admission. The framework is appropriate for the programmed access to the ATM machines for confirmed clients. The fingerprint and iris features of the client is verified and the corresponding client is given with the privilege to get to only when the currently extracted features generate the key points and using the generated key the features are matched with the features stored in the database.

4. MULTIPHASE SECURITY SOLUTIONS THROUGH LIFE CYCLE SECURITY :

Fraud migrates not just geographically but in multiple directions across ATM systems by compromising with multiple types of security as Physical Security, ATM card Security, Transactional and network Security, Authentication Security and User Security. A definitive objective of the lifecycle security is to make trusted, anchored condition for the entire ATM System. It is exceptionally fundamental and important to consider security from lifecycle perspective, with the end goal to screen and counter quickly relocating misrepresentation of very modern nature.

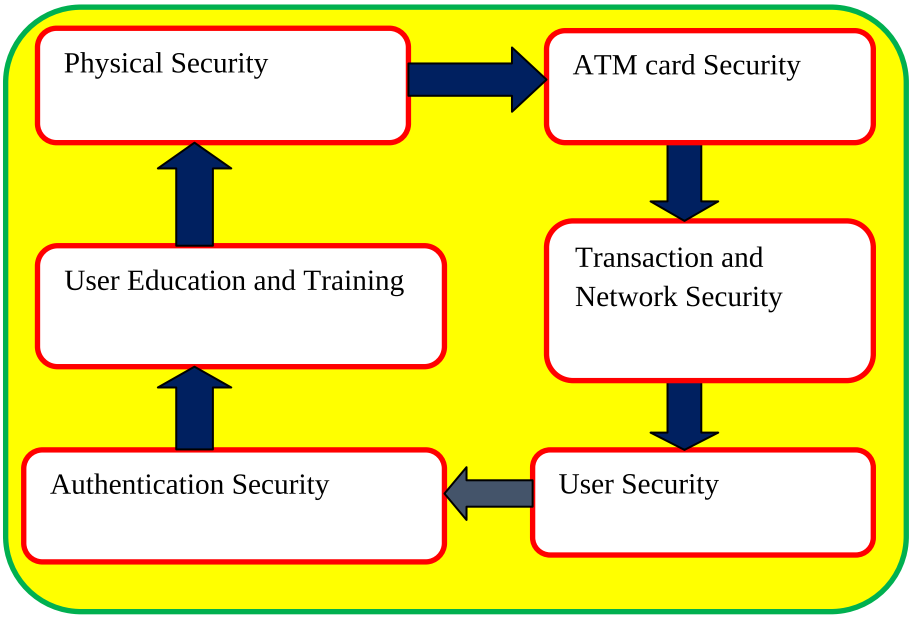

Figure-1: Lifecycle Security for ATM System

The term ATM System security life cycle refers to all interlinked stages for the functioning and operating of ATM machines and then identifies potential vulnerabilities or points which the fraudulent could target for an attack [12-18].

The qualitative data collection instrument chosen is the focus group. Four focus groups, each comprising of five members, are conducted. Group 1 comprised of 3 males/2 females, Group 2 consists of 2 males/3 females, and Group 3 consists of 4 males /1 female. Group 4 consists of 5 males only. Group 1, and Group 2 are chosen from the population of students and employees of Srinivas University, Mangalore, Group 3 and group 4 are chosen from the population of middle class people and business personals at Mangalore city of Karnataka.

Figure-1 provides visual representation of the lifecycle from a security viewpoint of mobile banking transactions. Even though lot of money have been spent on building and maintaining ATM systems, reports show that there exists potential vulnerabilities or attacks in different perspective, despite its availability anywhere. The lifecycle security for ATM system has different phases as Physical Security, ATM card Security, Transactional and Network Security, Authentication Security, User Security and User Education and Training, which is derived through focus group interaction.

Physical Security Phase

Physical Security is the security of ATM machine itself. In this sort of attack a truck is stacked with substantial development hardware to access the security nook and there by taking its money. Another kind of assault strategy is plofkraak is to take all opening of the ATM with silicon and fill the vault with hazardous gas or to put a touchy inside or adjacent to the ATM. This gas or hazardous is lighted and the vault is opened or mutilated by the power of the subsequent blast and culprits can break in. This is a standout amongst the most unsafe and genuine hazardous cause’s money lost as well as harms the close by condition. By utilizing diverse materials like revolving saw, blow burn, warm spear, and precious stone penetrate to fiercely open increasing direct access to money. This sort of assault is eluded as cutting. A few of the answers/solutions for physical attacks are examined in Table-1.

Table-1: Solutions to ATMs Physical Attacks

Physical attacks	Solutions
Ram-raiding, Plofkraak and Cutting	➢ A seismic/push locator alert ought to be fitted to the ATM safe body and safe entryway. ➢ A double reed attractive contact switch alert ought to be fitted to the entryway of the ATM Safe. ➢ A volumetric finder alert ought to be set on the mass of the ATM Secure Service Room. This ought to have the capacity to distinguish any development in the territory encompassing the ATM ➢ Profoundly complex multi point 3-dimensional camera ought to be fitted inside ATM focus. ➢ Warm sensors, seismic sensors, and hazardous identifier alert ought to be fitted ➢ A warmth/smoke sensor caution ought to be fitted inside the ATM. This ought to distinguish any type of oxy-acetylene or consuming bar assault on the ATM, and ought to be on the ATM security circuit. ➢ Individual Attack Alarms ought to be fitted in the ATM Secure Service Room as close as conceivable to the ATM. This is to give security to staff overhauling or the ATM. In the event that ATM's are in an open zone, at that point thought ought to be given to radio based individual assault caution ➢ Kerbs or comparative solid furniture's can be introduced before ATM machines and utilize a few obstructions that fold over ATM machines with the end goal to make lifting of ATM more troublesome. ➢ Exceedingly prepared Multiple security people

ATM Card Security Phase

ATM card security stage manages how to anchor from ATM Frauds. ATM Fraud is the taking the ATM card from the confirmed client. In the ATM attractive card data points of interest are endangered by a concealed card pursuer known as skimming gadget. The skimming gadget is typically introduced before card pursuer passage opening or at the ATM entryway bolt. Card Trapping is another technique for ATM card assault by setting wire, tapes or other system in the card passage space. The Thieves utilizes a plastic strip, embedded at the money machine to catch bank ATM cards is alluded as Lebanese circle.

Card catching and skimming is utilized just to trap and catch the physical ATM card however without stick they ready to get money from the record of others. With the end goal to get to PIN they utilize distinctive strategies like PIN Pad overlay-put a plastic stick cushion on the first one and content PIN when client enters, Spy Camera-by introducing counterfeit promoting box or blurbs with a little changed over camera inside to get the PIN, Powerful Telescope-scanners watch PIN passage action and judge the PIN from finger development amid activity and Honey Trap-put a false ad notice or administration hotline number planning to get PIN by help or suggestion. A portion of the answers for ATM card assaults are talked about in Table-2.

Table-2: Solutions to ATM Card Attacks

Types of ATM Fraud	Solutions
Card skimming	Anti skimming devices to prevent from capture of card information. Fascia scanning function to detect if any foreign objective attached.
Card Trapping	Use Jitter function along with card reader
PIN Attacks	• Fix Consumer awareness mirror to be aware of surroundings • Use fully covered tint glasses for ATM doors • PIN pad shield to prevent PIN compromised when entered • Utilize Specialized Bank commercial board appended with shrouded camera to watch presumed developments. • Use biometric identification along with PIN in order to access cash from ATM Systems.

Transaction and Network Security Phase

The security of ATM transactions and network mostly relies on the integrity of secure cryptoprocessor. When the customer information are transferred from respective authenticated financial institution to ATM machines should be in encrypted format. Customer Account information are encrypted using Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Wireless Transport Layer Security (WTLS) protocols. This implies that data is transmitted between Bank and ATM machines is kept secret (confidentiality) and that tampering will be detected (data integrity).

User Security Phase

For every single budgetary organization or financial institutions client/client security is one of greatest test in ATM frameworks. Budgetary organizations should more focus on the preventive proportion of obstruction enactment than on the issue of continuous constrained withdrawals. Client security Phase incorporates following measures.

- Use multiple cameras in different corner and centers of ATM counter which can record and store all the events.
- Use multiple security guards.
- Bank ought to embrace a crisis PIN framework for ATMs, where the client could ready to send a quiet alert in light of a risk.
- ATMs counter should display on-screen safety warnings and may also be fitted with convex mirrors above the display allowing the user to see what is happening behind them.
- On emergency, emergency telephone number switch should be installed all outside ATMs with in their jurisdiction. These will automatically connected to nearest police station
- Use different alarms at ATM doors, ATM machines and on the wall of the ATM Secure Service Room

Authentication Security Phase

User authentication is very important in ATM security system because even if ATM card is stolen un-authorized person unable to get to and get approved client records' money. Customer or User authentication is performed using multifactor authorization. It involves what you have, what you know, and what you are. What you know includes PIN. What you have include client mobile phone. Who you are requires biometric-facial recognisition. During account opening procedure user biometric identification is finished with the assistance of the geometry of the face (facial recognition) and mobile number is stored in bank along with user profile. Initially customer should enter PIN Number [18-33]. After entering PIN, when the customer facial recognisition is scanned through a scanner attached to ATM machines, it automatically generates every time distinct four digit OTP and that sent to customer authorized mobile through GSM connected to the microcontroller. Even though unauthorized person steals the ATM card, facial recognition cannot match. This process is explained through Figure-2.

Initially user enters ordinary PIN through the keypad of ATM machines. Simultaneously user facial recognition is made through facial recognisition scanning/identification system attached to ATM machines. PIN and facial recognition are sent to bank server and matched against stored PIN and facial recognition. If facial recognisition and PIN not matches then user is claimed as unauthorized user. If similarities are established then OTP is sent to the user registered mobile and again OTP is compared with stored OTP. If match is found then the user is claimed as authorized user, if not unauthorized user. Client's mobile acts as a token and generates OTP based on IMEI Number, IMSI number, hours, minute, day, year/month/date etc.

User Education and Training Phase

All the financial institutions should give proper education and training to its ATM customers. Educate cardholder how to choose a safe ATM, how to check physical surroundings, how to check ATM, and how to do when suspicious event happens. Following are the different tips to educate the customer.

- Don't reveal PIN
- Don't write PIN anywhere try to remember it
- Always pay close attention to the ATM and your surroundings. Don't select an ATM at the corner of a building
- Maintain an awareness of surroundings throughout the entire transaction.
- Do not use an ATM that appears unusual looking.
- Do not allow people to look over user shoulder as user enters PIN.
- Do not wear expensive jewelry or take other valuables to the ATM.
- Never count cash at the machine or in public.
- Maintain a supply of deposit envelopes at home or in car. Prepare all transaction paperwork prior to arrival at the ATM. This will limit the measure of time spent at the machine.
- Closely monitor bank statements, as well as balances, and immediately report any problems to bank.
- If card is stolen immediately report to bank and give complaint to police station

5. ANALYSIS OF THE LIFE CYCLE SECURITY MODEL :

A SWOT Analysis is a compelling apparatus which can be utilized to look at the issues which will straightforwardly influence the achievement of new Model. In these examination quality/strengths, shortcoming/weakness, opportunity and risk/threat of the model are talked about.

Strengths:

- ➢ Difficult to hack/crack the system security
- ➢ Ensures that ATM system is continues to operated with in trusted environment
- ➢ Minimizes the risk of fraud
- ➢ Cancel out points of entry of the fraudster into the ATM system operating environment
- ➢ Improves User Trust over ATM machines
- ➢ Secured messages and transactions that contains sensitive customer data
- ➢ Increased accuracy of online banking transactions Through ATMs
- ➢ Creates security awareness to end users
- ➢ Higher User Authentication security
- ➢ Even though card is stolen and theft gets the PIN and Mobile, cannot gain access to account due to mismatch of facial recognition
- ➢ Banking services at any time

Weakness:

- Requirement of high memory and processors at Bank's servers
- Transaction duration time increases.
- Lack of technology support
- Initial investment in technology will be expensive
- Lack of trained security guard

Opportunities:

- The ability to obtain a larger customer base due to higher security
- The ability to take advantage of the growing popularity of online banking through ATM channel
- Improves consumer reputation of the technology

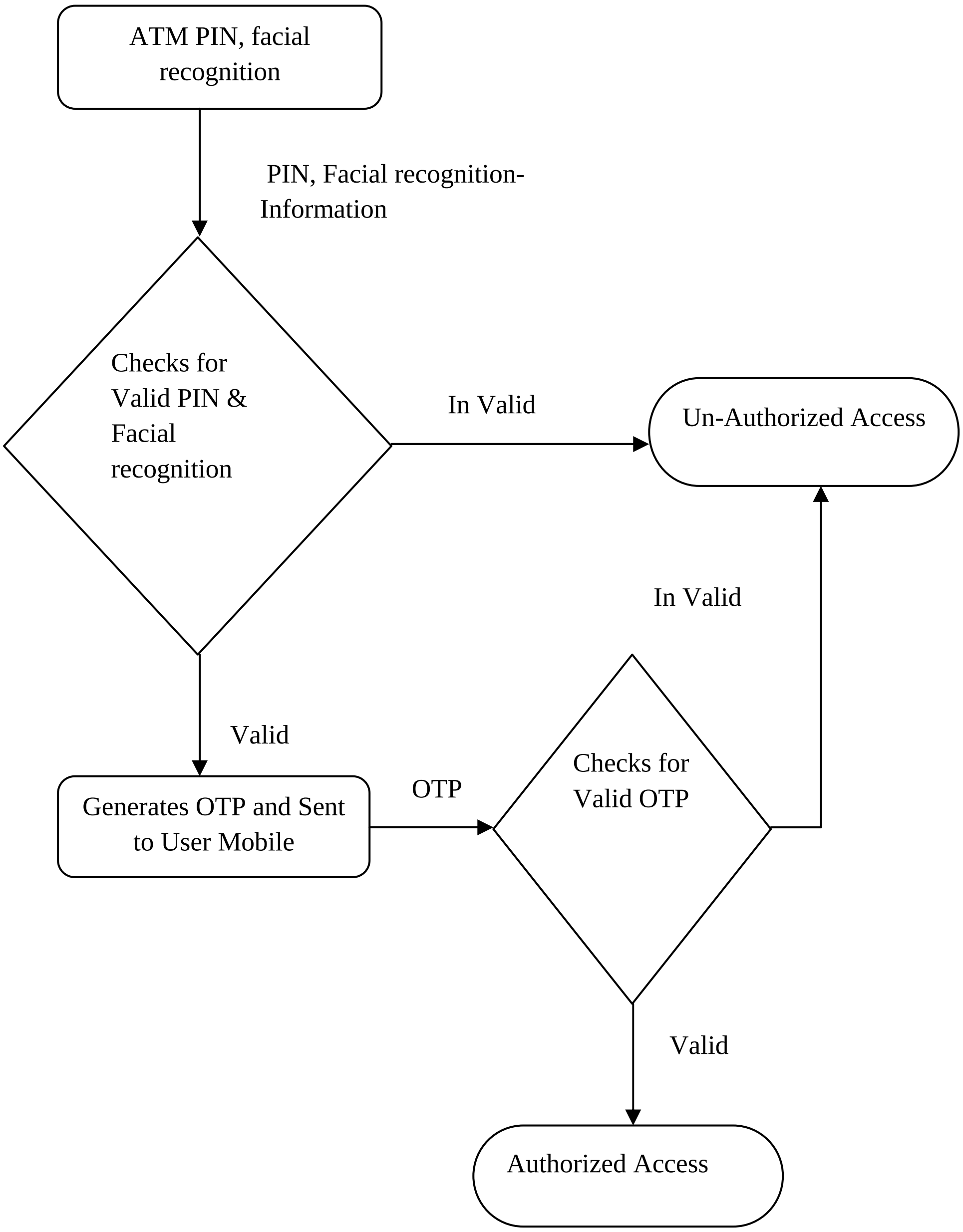
ATM PIN, facial recognition
PIN, Facial recognition-Information
Checks for Valid PIN & Facial recognition
In Valid
Un-Authorized Access
In Valid
Valid
Generates OTP and Sent to User Mobile
OTP
Checks for Valid OTP
Valid
Authorized Access

Figure-2: User Authentication security Process

- Enhances reputation of the bank or any other financial institutions by providing secured services to its customer
- Global expansion of banking services due to high security

Threats:

- Possible failure of products due to non-acceptance of customer
- General competitiveness of the banking industry
- Lack of newer technology support

6. CONCLUSION :

This paper investigated the security threats of ATM systems in a high-level, co-coordinated way, at all the phases along the lifecycle, constantly assessing crime migration patterns and risks. The talks support to fabricate applications for ATMs that guarantee clients can safely do exchanges at ATM counters. The security lifecycle appears as a series of phases where different kinds of protection are essential at different points along the lifecycle to prevent fraudulent transactions and to reduce any types of risk. A lifecycle approach including different phases as Physical Security, ATM card Security, Transactional and Network Security, Authentication Security, User Security and User Education and Training aims to cancel out points of entry of the fraudster into online financial transaction environment. The multilevel authentication used by the User authentication phase helps to provide rigid security solutions to identify authorized customer. The Customer Education and Training help to aware ATM and their security measures and improve their confidence over ATMs. The SWOT analysis of the Lifecycle Security Model helps to know the strength, weakness, opportunities and threats/challenges with special concern to bank ATM transactions.

REFERENCES :

[1] Onyesolu, M. O., & Ezeani, I. M. (2012). ATM Security Using Fingerprint Biometric Identifier: An Investigative Study. *IJACSA) International Journal of Advanced Computer Science and Applications*, *3*(4), 68-72.

[2] Das, S., & Debbarma, J. (2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system. *International Journal of Information and Communication Technology Research*, *1*(5), 197-203.

[3] Wan, W. W., Luk, C. L., & Chow, C. W. (2005). Customers' adoption of banking channels in Hong Kong. *International Journal of bank marketing*, *23*(3), 255-272.

[4] De Luca, A., Langheinrich, M., & Hussmann, H. (2010). Towards understanding ATM security: a field study of real world ATM use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 16). ACM.

[5] Boateng, R. (1970). Developing e-Banking capabilities in a Ghanaian Bank: Preliminary lessons. *The Journal of Internet Banking and Commerce*, 11(2), 1-11.

[6] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, *40*(3), 614-634.

[7] Turban, E., King, D., Lee, J. & Viehland, D. (2004). Electronic Commerce: A Managerial Perspective 2004, International Edition. Pearson Prentice Hall, Upper Saddle River, NJ, USA.

[8] Raina, K. & Harsh, A. (2002). M-commerce Security. *Osborne*, New York, NY, USA.

[9] Shaikh, S. A., & Rabaiotti, J. R. (2010). Characteristic trade-offs in designing large-scale biometric-based identity management systems. *Journal of Network and Computer Applications*, 33(3), 342-351.

[10] Krishnamurthy, P., & Redddy, M. M. (2012). Implementation of ATM Security by Using Fingerprint recognition and GSM. *International Journal of Electronics Communication and Computer Engineering*, 3(1), 1-4.

[11] Onyesolu, M. O., & Ezeani, I. M. (2012). ATM Security Using Fingerprint Biometric Identifer: An Investigative Study. *IJACSA) International Journal of Advanced Computer Science and Applications*, 3(4), 68-72.

[12] Krishna Prasad, K. and Aithal, P.S. (2017). A Study on Online Education Model Using Location Based Adaptive Mobile Learning. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *1*(1), 36-44. DOI: http://doi.org/10.5281/zenodo.820457.

[13] Krishna Prasad, K. & Aithal, P.S. (2017). A Customized and Flexible Ideal Mobile Banking System Using 5G Technology. *International Journal of Management, Technology, and Social Sciences (IJMTS),*1(1), 25-37. DOI: http://doi.org/10.5281/zenodo.820457.

[14] Krishna Prasad, K. & Aithal, P.S. (2016). The Growth of 4G Technologies in India- Challenges and Opportunities. *International Journal of Management, IT and Engineering (IJMIE), 6*(1), 543-551. DOI : http://doi.org/10.5281/zenodo.161130.

[15] Krishna Prasad, K. & Aithal, P.S. (2016). Changing Perspectives of Mobile Information Communication Technologies towards Customized and Secured Services through 5G & 6G. *International Journal of Engineering Research and Modern Education, 1*(2), 2016, 210-224.

[16] Krishna Prasad, K. & Aithal, P.S. (2016). An Online Comparative Study on 4G Technologies Service Providers in India. *International Journal of Advanced Trends in Engineering and Technology (IJATET), 1*(1), 96-101. DOI: http://doi.org/10.5281/zenodo.240269.

[17] Krishna Prasad, K. & Aithal, P.S. (2015). Mobile System for Customized and Ubiquitous Learning by 4G/5G. *International Journal of Management, IT and Engineering (IJMIE),* 5(7), 63-71.

[18] Krishna Prasad, K. & Aithal, P.S. (2015). Massive Growth of Banking Technology with the aid of 5G Technologies. *International Journal of Management, IT and Engineering (IJMIE),* 5(7), 616-627.

[19] Krishna Prasad, K. & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE),* 1(2), 86-92. DOI: http://dx.doi.org/10.5281/zenodo.1130581.

[20] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML), 1*(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678.

[21] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS), 2*(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608.

[22] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS), 2*(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191.

[23] Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML), 1*(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653.

[24] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML), 1*(2), 51-65. DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[25] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *1*(2), 98-111. DOI: http://dx.doi.org/10.5281/zenodo.1067110.

[26] Krishna Prasad, K. & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation using Euclidean Distance for Identifying a User. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *2*(2), 116-126. DOI: http://doi.org/10.5281/zenodo.1133545.

[27] Krishna Prasad, K. & Aithal, P.S. (2018). An Alternative Approach to Fingerprint Hash Code Generation based on Modified Filtering Techniques**.** *International Journal of Innovative Research in Management, Engineering and Technology*, *2*(12), 1-13. DOI: IJIRMET1602012001.

[28] Krishna Prasad, K. & Aithal, P.S. (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. *International Journal of Advanced Trends in Engineering and Technology*, *3*(1), 1-11. DOI : http://doi.org/10.5281/zenodo.1135255.

[29] Krishna Prasad, K. & Aithal, P.S. (2018). A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code. *International Journal of Computational Research and Development*. *3*(1), 13-22. DOI: http://doi.org/10.5281/zenodo.1144555.

[30] Krishna Prasad, K. & Aithal, P.S. (2018). A Comparative Study on Fingerprint Hash Code, OTP, and Password based Multifactor Authentication Model with an Ideal System and Existing Systems. *International Journal of Applied and Advanced Scientific Research,* 3(1), 18-32. DOI: http://doi.org/10.5281/zenodo.1149587.

[31] Krishna Prasad, K. & Aithal, P.S. (2018). A Novel Tuning Based Contrast Adjustment Algorithm for Grayscale Fingerprint Image. *Saudi Journal of Engineering and Technology (SJEAT)*, 3(1), 15-23. DOI: http://10.21276/sjeat.2018.3.1.3.

[32] Krishna Prasad, K. & Aithal, P.S. (2018). ABCD Analysis of Fingerprint Hash Code, Password and OTP based Multifactor Authentication Model. *Saudi Journal of Business and Management Studies*, 3(1), 65-80. DOI: http://10.21276/sjbms.2018.3.1.10.

[33] Krishna Prasad, K. & Aithal, P.S. (2018). A Study on Pre and Post Processing of Fingerprint Thinned Image to Remove Spurious Minutiae from Minutiae Table**.** *International Journal of Current Research and Modern Education*, 3(1), 197-212. DOI: http://doi.org/10.5281/zenodo.1174543.

****