Saudi Journal of Business and Management Studies (SJBMS) **ISSN 2415-6663 (Print)**
Scholars Middle East Publishers **ISSN 2415-6671 (Online)**
Dubai, United Arab Emirates
Website: http://scholarsmepub.com/

ABCD Analysis of Fingerprint Hash Code, Password and OTP Based Multifactor Authentication Model

Krishna Prasad K[1] , P. S. AITHAL[2]
[1]Research Scholar, College of Computer and Information Science, Srinivas University, Mangaluru, Karnataka, India.
[2]College of Computer and Information Science, Srinivas University, Mangaluru, Karnataka, India.

***Corresponding author**
Krishna Prasad K

Article History
Received: 10.01.2018
Accepted: 20.01.2018
Published: 30.01.2018

DOI:
10.21276/sjbms.2018.3.1.10

Abstract: Authentication is the usage of one or multiple mechanisms to show that who you declare or claim to be. Authentication ensures that users are granted to some resources or services after verifying their identity. The essential characteristics of every authentication system are to provide high security for their users. Multifactor authentication model always improves or enhances the security compared to single-factor authentication model. This new model makes use of three factors-biometric Fingerprint Hash code, One Time Password (OTP), and Password. Fingerprints are not fully secret compare to passwords, because if passwords are leaked which can be easily revocable using another password and which is not true in case of fingerprint biometric security system. If an authentication system uses only fingerprint biometric features, it is not easy to change fingerprint, because fingerprint is static biometric, which never change much throughout the lifespan. In this paper, as per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, (5) Performance Evaluation matrix Issues. The constituent critical elements of Multifactor Authentication model determinant issues are listed under the four constructs - advantages, benefits, constraints and disadvantages of the ABCD technique and tabulated. The analysis has brought out many critical constituent elements, which is one of the proofs for the success of the new methodology.
Keywords: Multifactor Authentication Model, Fingerprint Hash Code, ABCD analysis, Constituent Critical Elements.

INTRODUCTION

By definition, authentication is using one or multiple mechanisms to show that who you declare or claim to be. As soon as the identity of the human or machine is demonstrated, then human or machine is authorized to grant some services. Three worldwide referred authentication process are (1) Token supported authentication, (2) Biometric supported authentication, and (3) Knowledge supported authentication.

Token supported authentication makes use of key cards, bank cards, and smart cards. Token supported authentication system sometimes uses knowledge supported techniques to improve security. Biometric supported authentication strategies, together with fingerprints, iris scan and facial reputation aren't yet extensively adopted [1, 2]. The essential flaws of this technique are that such systems can be costly, and the identification process may be slow and regularly unreliable. However, this form of technique presents the highest level of protection. Knowledge supported authentication is most commonly and widely used authentication technique and encompass both text-based and image-based passwords. The image-based techniques can be further subdivided into two classes: recognition-primarily based and recall based graphical techniques. The use of recognition based strategies, a person is provided with a set of images and the user is authenticated through recognizing and identifying the images, which is registered at the time of registration process. In recall based techniques it's essential that user has to reproduce something like a pattern, which is created or drawn at the time of registration process.

One time password can be generated in two forms. (1) Time-synchronized OTP: In time-synchronized OTPs the person has to enter the password within a time frame or within a stipulated time, in other words, OTP having lifespan only for few amount of time after that time it will get expired and another OTP will be generated. (2) Counter-synchronized OTP: In Counter-synchronized OTP, instead of regenerating OTP after the stipulated time, a counter variable is coordinated or synchronized between client device and server.

Automatic Fingerprint Identification System (AFIS) consists of different techniques like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [3-10]. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or readers. There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause a difference in Hash code [11-14]. Based on the different Methods of Fingerprint Hash code generation, it reveals that fingerprint hash code does not suit exclusively for authentication or security purpose. But it uniquely identifies an individual person or human being through a Hash code key.

It is well known that we can improve the performance of any system by comparing it with a hypothetical, predicted system of that kind called Ideal system [15]. The word Ideal system refers to the system which has utmost characteristics, which cannot be improved further. It is what our mind tells ultimate and which reached the pinnacle of success in the respective field, which can be compared to all other systems of similar type, which lacks in some qualities [16]. The less-efficient system can be converted into the ideal system with the aid of research and continuous innovation in that field. Many objects we can consider as ideals like an ideal gas, ideal fluid, ideal engine, ideal switch, ideal voltage source, ideal current source, ideal semiconductor and ideal communication technology and all of these are considered as standards to improve the quality and performance of similar type. Recently many ideal systems are studied, which includes ideal business system [16], ideal education system [17-20], ideal technology system [15], ideal strategy [21], ideal energy source [22], ideal library system [23], ideal banking system [24, 25], ideal software [26], ideal optical limiter [27], ideal analysis model [28] and ideal mobile banking system [29]. The ideal system of any kind can be placed in mind, while improving the characteristics of practical devices/ systems and reach ideal system or considered to be a pinnacle of success. Some of the ideal systems with respect to Authentication System are listed in Table-1.

Table-1: List of Ideal components with respect to Authentication System

SL. No	Ideal System Components/ Characteristics	Definition of Ideal Systems Components/ Characteristics
1	Ideal Speed	The time taken by the Automatic Verification or Authentication System to authenticate the registered user.
2	Ideal Data Transfer Rate	Any amount of data can be transferred from source to destination without any delay or within null unit of time duration (In client Server Model)
3	Ideal Signalling efficiency	The quality of signal is 100% efficient in all aspects.
4	Ideal Security	100% protection of Registered user means no intruder can able to break the system anyway.
5	Ideal Availability	Service can be available any part of the world anytime.
6	Ideal Bandwidth	The volume of Information per unit of time that a system can handle is unlimited or uncountable.
7	Ideal False Acceptance Rate	The percentage of system incorrectly classifies the input pattern to an unregistered user is zero.
8	Ideal False Rejection Rate	The probability that the Authentication framework unable to identify a match between the authentic people is always zero.
9	Ideal Equal Error Rate	Acceptance and rejection mistakes are identical in the system and which is equal to zero.
10	Ideal Failure to Enroll Rate	The unsuccessful attempt made to enrol in database or template of an Automatic Fingerprint Identification System by the input is zero.
11	Ideal Accuracy Rate	Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high.

In this paper, a new Multifactor Authentication Model based on Fingerprint Hash Code, Password, and OTP is discussed. In this model fingerprint Hash code is used as index-key or identity key. Initially, the user loads static Fingerprint image and which is converted to Hash Code through the programme. Later time synchronized OTP is checked and verified and the last password is prompted by the server and verified by the server. Finally, the password is prompted and verified by the server. The remaining part of the paper is organized as follows. Section 2 explains about ABCD Model. Section 3 describes Multifactor Authentication model. Section 4 describes OTP generation. Section 5 describes ABCD analysis of new Multifactor

Authentication Model. Section 6 identifies the critical constituent elements of these determinant factors. Section 7 concludes the paper.

ABCD Analysis Framework

Many techniques are available in the literature, to investigate the individual characteristics, system traits, and effectiveness of an idea or concept, the effectiveness of a method to know its merits and demerits and also business value in the society. The individual traits or organizational effectiveness & techniques in a given surroundings may be studied the usage of SWOT analysis, SWOC evaluation, PEST analysis, McKinsey7s framework, ICDT version, Portor's 5 force model and so on. Recently a new model is introduced to these analysis areas called ABCD analysis framework [30], which is used for analyzing business concept, business system, new technology, new model, new idea/concept etc. In the qualitative evaluation the use of ABCD framework, the new idea or new system or new strategy or new generation or new model or new concept is further analyzed studied or analyzed using critical constituent elements. In the quantitative evaluation the use of ABCD framework [31], can be used to assign appropriate score or rating for each critical constituent elements, which is calculated through empirical research. The final score is calculated and based on the score the new idea or new system or new strategy or new generation or new model or new concept can be accepted or rejected. Consequently, ABCD evaluation framework may be used as a research tool in these regions and is easy but systematic study or analyzing method is essential for business concept or systems or models or ideas or strategy evaluation [30-46].

Multifactor Authentication Model Using Fingerprint Hash Code, OTP, and Password

Figure-1 shows Dataflow Diagram of Multifactor Authentication model used in this study. Initially on the client side using an interface user loads fingerprint image into the system. First, using Euclidean distance fingerprint image features are extracted, which is explained in Section 3 and 4.

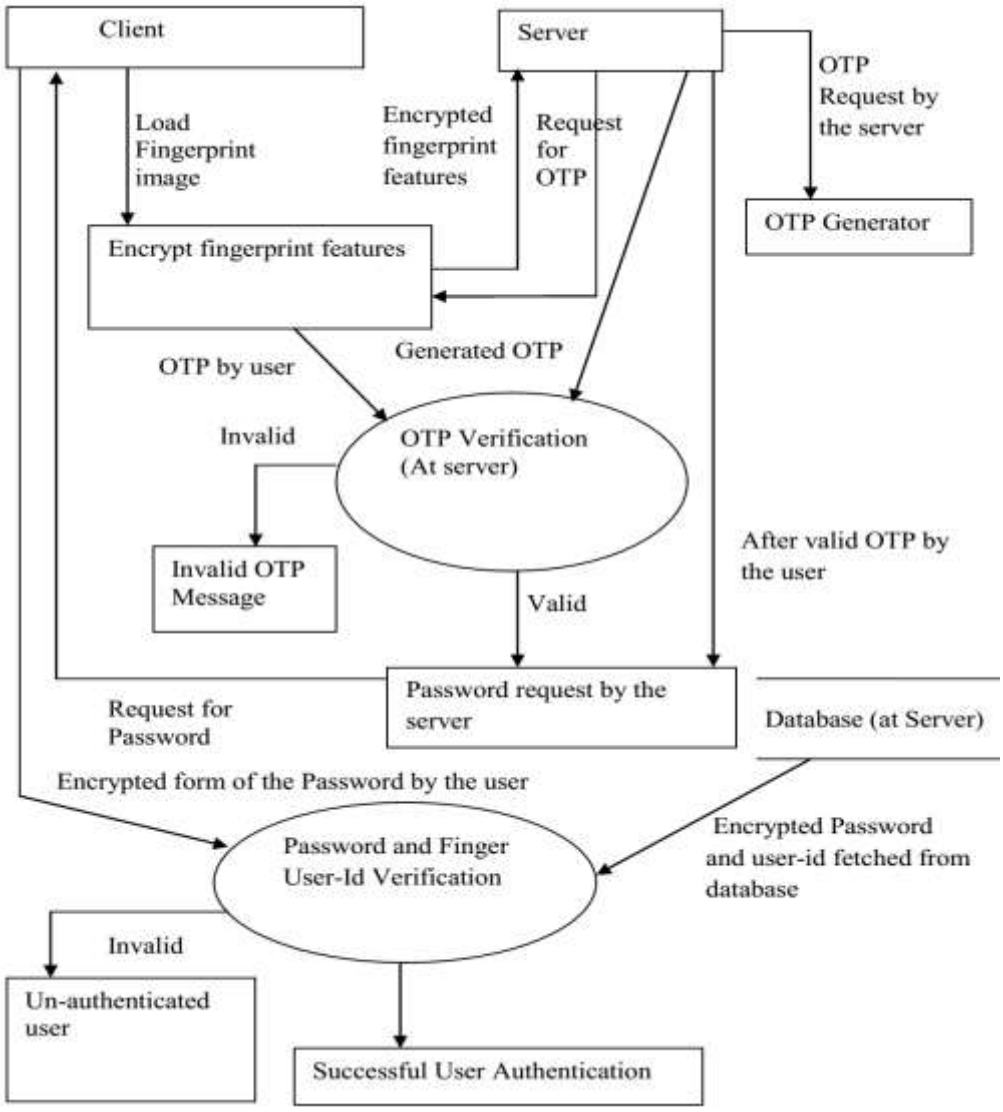

Fig-1: Dataflow Diagram of Proposed Multifactor Authentication

These features are encrypted and sent to the server. As soon as these features arrive at a server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered mobile phone user. Client system prompts a message to enter OTP, which is received to the registered mobile phone of the user.

The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side. If OTP is verified, server requests for the password, the user enters the password through a client-side interface and entered password reaches to the server. The server verifies the user entered a password with the already stored password in its database. Since database password is stored in encrypted format. The password which is stored in the database in encrypted form and finger user-id hash code is encrypted one again to enhance security.

So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match them user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Password, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered an unauthorized user. If OTP not matches then the user is blocked from further steps in the authentication process. In this research study, this is not implemented as server and client in different machines. The model of this approach is implemented on the same machine using MATLAB 2015a.

One Time Password Generator

In this research work, One Time Password Generator is responsible for generating OTP. This is a function located on the server. In this study, Time synchronized OTP is generated by combining some features. The time for which OTP is valid is administrative specific, for simplicity we consider in this work as 2 minutes. The algorithm for generating OTP is explained below.

Algorithm:

Step-1: Generate the Hash code for input fingerprint using MD5 Hash Function.
Step-2: Extract system Date and Time.
Step-3: Extract seconds separately.
Step-4: Consider only integer part of the seconds.
Step-5: A 4 × 4 sized matrices of the random number is generated.
Step-6: Date and Time are converted into string data type.
Step-7: Random matrix is concatenated with Date and Time string.
Step-8: Hash code of the input fingerprint image is concatenated with result of Step-7.
Step-9: Hash code is generated for combined string obtained from Step-8.
Step-10: A random number is generated between1 to 32.
Step-11: If the random number is in between 1 to 8 (including both) then extracts first 8 characters of the Hash code of size 32 characters generated in Step-8.
Step-12: If the random number is in between 9 to 16 (including both) then extract next 8 characters (from position 9 to 16) of the Hash code of size 32 characters generated in Step-8.
Step-13: If the random number is in between 17 to 24 (including both) then extract next 8 characters from position 17 to 24) of the Hash code of size 32 characters generated in Step-8.
Step 14: If the random number is in between 24 to 32 (including both) then extract next 8 characters from position 24 to 32) of the Hash code of size 32 characters generated in Step-8.

ABCD Analysis of Multifactor Authentication Model

Multifactor Authentication Model used in this research work can be analyzed using ABCD Analysis Aithal, P. S. *et al*., [30], proposed ABCD analyzing framework to analyze a new model to observe and understand its effectiveness in imparting value to its stakeholders. The ABCD analysis effects in an organized listing of Business or new Model with advantages, Benefits, constraints, and disadvantages in a systematic way or form. The complete framework is divided into various issues, the area which new model is focused. Various key properties and affecting the area of the new model may be identified and analyzed under each area of issues identified before.

Later some of the critical constituent element for each identified issue is recognized and analyzed and which is shown in Figure 2. This method of analysis is simple and also offers a guideline to identify and examine the effectiveness of the new model in this context. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, (5) Performance Evaluation matrix Issues.

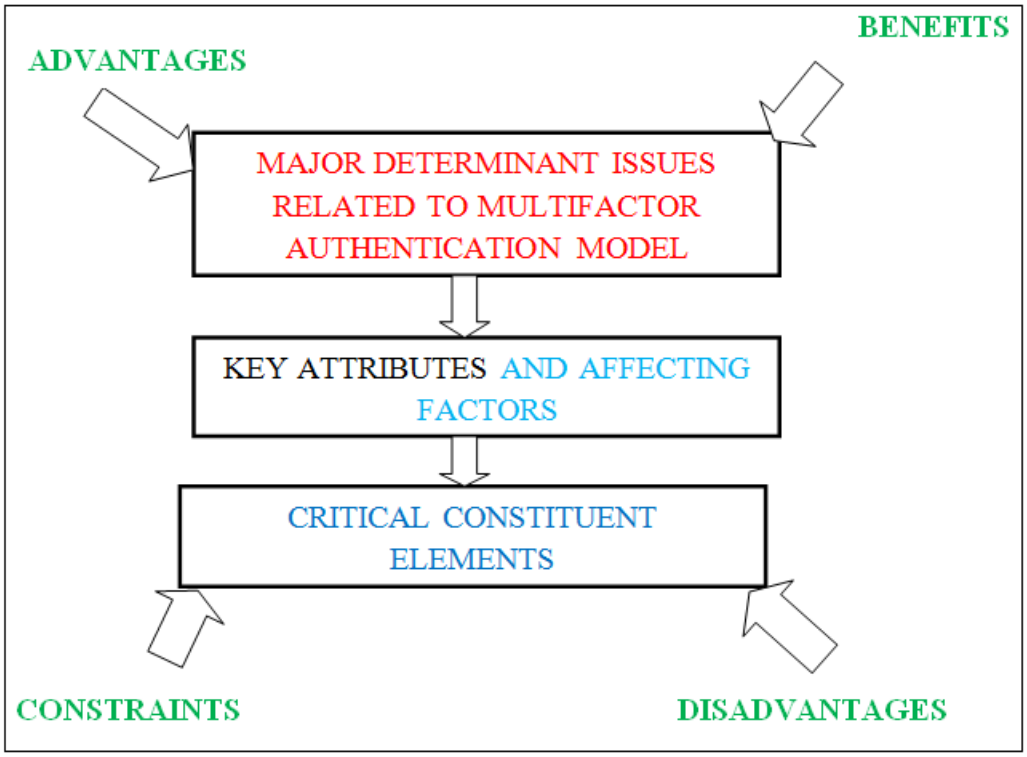

Fig-2: Block diagram of Issues affecting the Fingerprint Hash code, Password, OTP based Multifactor Authentication Model

(1) Security Issues

Security is very important in the Authentication process. An ideal security refers that a system which is impossible for an intruder to break or impossible for the unregistered user to access the system. In the Authentication process, security refers safeguarding the user personal data used for the authentication process, which includes, Fingerprint Hash code, Password, One Time Password (OTP). The affecting factors of Security issues include Fingerprint Hash code, Password, and OTP under key properties or levels like user level, network level, and Database or template level are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(2) User-friendly Issues

The user-friendliness of Multifactor Authentication Model signifies that user should able to get access to the system effortless or easily without remembering anything or very minimum amount of data. The affecting factors under key properties like Response time, Access time, Automatic Process, Speed, and Availability are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(3) Input Issues

Input ensures that registered user should able to get access to the system or authenticated with very less or no input or automatically. The affecting factors under key properties like Minimum Possession, Least input, Input Selectivity, Ubiquitous Data, Reliability, Usability, Efficiency, Input security and execution time are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(4) Process Issues

Process Issues ensures that user should able to complete authentication process without any fault, fast and completely. The affecting factors under key properties like Atomicity, Consistency, Isolation, Availability, effort free, and High durability are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(5) Performance Evaluation matrix issues refer all the performance evaluation matrices normally used for the authentication system. The affecting factors under key properties like False Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to enroll rate, Accuracy Rate, and Execution are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

Each determinant issue has sub-issues called key attributes used for analyzing the advantages, benefits, constraints and disadvantages, the four constructs of the framework.

The factors affecting the various determinant issues of Multifactor Authentication Model for each key

attributes under four constructs are derived by a qualitative data collection instrument namely, focus group method and are listed in Table-2.

Table-2: Analysis of Fingerprint Hash code, Password, and OTP-Multifactor Authentication Model for Verification purpose

Determinant Issues	Key Attributes	Advantages	Benefits	Constraints	Disadvantages
Security Issues	User level security (For Biometric Image-Hash code)	Easy to secure using personal devices like mobile phone, Laptop, USB drive, and private cloud drive	increases demand Cloud Drive, Mobile, Pen drive, and laptop	High Security of the Cloud Drive, USB device, Laptop, and Mobile Phone is questionable	Acceptance by the user
	Network Level Security	Non- reversible, Non- Revocable Hash code,	Customer faith increases Can attract new customer	tampering of data	Network failure due to some uncontrollable circumstances
	Database or Template Security	Single Hash value is used for comparing, Non revertible Hash code	Efficient memory use, Database is easily manageable	Database table requires values in Hash form	Database failure, Server failure
User-friendly Issues	Response time	Increased rate of growth of authentication process	Increased customer pool	Requires high configuration system and efficient algorithms	Hardware and Software cost
	Access time	User Instantaneous authentication	Reduced Queuing, Reduced waiting process	Requires good network, memory, and processor	Hardware and software cost
	Speed	Increased Authentication request per unit time	Increased customer satisfaction, retention and acquiring new customers becomes easy	Requires high configured system and reduced time complexity	Hardware and software cost, High bandwidth network,
	Automatic process	Minimum prior information of the system required	Increased customer satisfaction,	Ability to make difference between registered and unregistered user, processing power	Utilization of the hardware and software resources are too high complex backend design of user interface
	Availability	Ubiquitous authentication	Reduced request queue	Dedicated server and network	24 × 7 working server
Input Issues	Minimum Possession	minimum knowledge parameters required for authentication	User get authenticated anywhere without carrying anything	Capacity of the system to differentiate between registered user and intruder with minimum data	Lack of information
	Minimum input	Simple User authentication from customer point of view	Reduced I/O operation	Requirement of unique and robust parameter for user Authentication	Lack of information
	Input Selectivity	Reduced error in inputting	Increased Customer comfort and satisfaction	User ability to identify correct image	Negligence of the user in selection of input
	Ubiquitous	Ubiquitous	Increased user	Requirement of	Misuse of

	input	Authentication process	satisfaction	high configuration system and network availability	Authentication system, More intruder will try to break the system
	Reliability	Improved consistency of the system	Improved user satisfaction	Operating cost	Significant startup and Maintenance cost
	Usability	One parameter for multipurpose like fingerprint image	Reduced parameter requirement for authentication	The ability of the software to make distinction between different context of the same parameter	Intruder or un-registered user tries to get multipurpose parameter used in the authentication process.
	Efficiency	Increased number of requests	Accurate results, error- free output	Quality of the input	Inability to handle error- prone or partial input
	Security	User personal data protection	Trust and faith over system increases	Uniqueness, permanence, Universality, and revocability	Cost of the system becomes high.
	Execution time	Increased growth rate in authentication	Trust and faith over system increases	Requires good time and space complexity algorithm	Requirement of Good configuration system increases cost
Process Issues	Atomicity	Authentication process Rollback or Commit at the time of system failure	Authentication failure is very rare or practically zero.	Need of good fault tolerance techniques.	Requires separate programme for database protection /safeguards
	Consistency	Ensures consistent state at the time of system failure	Authentication process ensures consistency,	Need of good fault tolerance techniques.	Database management and safe guarding requires extra efforts and cost
	Isolation	Authentication process gets isolation property	Enhanced user trust and satisfaction	Need for good lock-based concurrency control system	Database management and lock-based concurrency control requires extra cost
	Availability	Ubiquitous authentication	Reduced request queue	Dedicated server and network	24 × 7 working server
	Effort free	User freely and easily interacts with authentication system	User enjoys working with system, Increased user trust, and satisfaction	Requires navigational and narrative user interface, Input should be selective rather than enter	Complex design of user interface and programme increases cost
	Durability	Changed Password and Biometric-ID durable for long time	Revocability can be done easily, if password or finger-id is compromised	Need of good fault tolerance techniques.	Database management and safeguarding requires extra efforts and cost
Performance Evaluation matrix issues	False acceptance rate	The ability of the system to differentiate registered and the unregistered user can be tested.	Improved biometric matching and identification rate	The fingerprint unique property	Not useful to identify the performance of non-biometric factors.

	False Rejection Rate	Ability of Authentication system to identify registered user can be improved	Biometric Matching rate and registered user identification can be improved	Unique fingerprint feature should be used for registered user identification	Not useful to identify performance of non-biometric factors
	Equal Error Rate	Ability of Authentication system to identify rejection and acceptance rate can be easily studied	Biometric Matching rate, registered user, and un-registered user identification error can be improved	Unique fingerprint feature should be used for registered and unregistered user identification	Not useful to identify performance of non-biometric factors like password
	Failure to enroll rate	The capacity of the authentication system in identifying person when some specific features are missing can be studied easily	Biometric matching rate, enroll rate failure can be improved	Sophisticated feature enhancement techniques are essential	Not useful to identify performance of non-biometric factors
	Accuracy Rate	The overall matching performance and accuracy can be easily studied	Overall quality of matching can be studied, analyzed, and improved	Sophisticated filtering, feature enhancement techniques are essential Good false rejection and acceptance rate are compulsory	Not useful to identify performance of non-biometric factors
	Execution time	The rate of users get authenticated increases per unit time.	Trust and faith over system increases	Requires good time and space complexity algorithm	Requirement of Good configuration system increases cost

Critical Constituent Elements as per ABCD Model

The important constituent factors of determinant issues are listed beneath the four constructs - advantages, benefits, constraints and disadvantages of the ABC model and tabulated in Tables-3 to 6.

Table-3: Advantages of Multifactor Authentication Model for Verification purpose

Sl. No	**Issue**	**Factors affecting**	**Critical Constituent Elements**
1	Security Issues	Mobile/Smart Phone	Structure of locking pattern
			Password strength
		USB-pen Drive	Password strength of third-party software
			Usage of USB (Public/ Private)
		Laptop	Password strength
		Private cloud drive	Security strength of cloud drive
			Accessibility strength of image by programme/software
		Non-reversible Hash code in network level	Strength of cryptographic programs/ Hash code in network level
		Revocable Hash code	Ability or how fast the system having capacity to change password and finger-id, when compromised
		Non-reversible Hash code in network level	Strength of cryptographic programs/ Hash code in template level
2	User-friendly issues	Increased rate of growth of authentication process	Conversion time required to convert fingerprint image to hash-id
			Time required for fetching password and

			decrypting
			Network speed for OTP
			Speed of Matching function
		Increased Authentication request per unit time	Ability of concurrent authentication
			Efficiency of Hash code matching rate
		Minimum prior information of the system required	The ability of the system to authenticate without prompting anything or with minimum input (only by selection or automatic)
		Ubiquitous authentication in user-friendly issue	The system used for authentication
			Availability of network
3	Input Issues	Minimum Knowledge parameters	The ability of the system to authenticate without prompting or without accepting more input from the user. (only password)
		Simple User authentication from customer point of view	Number of Input
			Narration used in the interface
		Reduced error in inputting	The way the input are provided to the system (Selection rather than entering)
		Ubiquitous Authentication process in input	The device used for authentication process
			Availability of network
		Consistency of the system	Reliability of the system
			The working efficiency of the system
		Multipurpose parameter	The ability of the unique fingerprint features to make different actions in different instances
		Increased number of requests	The execution time of the system
			Features or quality of input
		User personal data protection	Security mechanisms used in authentication process
			Security used for protecting input
		Increased growth rate in authentication due to input	The structure of the input
			Execution time of the algorithm used (time complexity)
4	Process Issues	Authentication process Rollback or Commit at the time of system failure	Strength of RDBMS
			RDBMS transaction atomicity property
		Ensures consistent state at the time of system failure	Strength of RDBMS
			RDBMS transaction consistent property
		Authentication process gets isolation property	Strength of RDBMS
		Ubiquitous authentication in process issue	RDBMS transaction atomicity property
			The device used for authentication process
			Availability of network
		User freely and easily interacts with authentication system	Simple user interface
			Navigational and narrative interface
		Changed Password and Biometric-ID durable for a long time	Management and maintenance of Database
			Safeguarding of database
5	Performance Evaluation matrix issues	The Ability of the system to differentiate registered and the unregistered user can be tested.	The fingerprint image unique feature
			Quality of the fingerprint image
			False Acceptance Rate
		The Ability of Authentication system to identify registered user can be improved	The fingerprint image unique feature
			Quality of the fingerprint image
			False Rejection Rate
		The Ability of Authentication system to identify, reject and accept a fingerprint image can be easily studied	The fingerprint image unique feature
			Quality of fingerprint image
			Difference between Acceptance and Rejection Rate
		The capacity of the authentication system in identifying person when some specific features are missing can be studied easily	The fingerprint image unique feature
			Quality of the fingerprint image
			Ability of the system to convert hash code

			from partial fingerprint image
		The overall matching performance and accuracy can be easily studied	The fingerprint image unique feature
			Quality of the fingerprint image
			Rejection rate
			Acceptance rate
		Increased growth rate in authentication due to performance issue	The structure of the input
			Execution time of the algorithm used (time complexity)

Table-4: Benefits of Multifactor Authentication Model for Verification purpose

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	Increases demand Cloud Drive, Mobile, Pen drive, and laptop	Usage of cloud drive for authentication process
			Usage of mobile phone for authentication process
			Usage of pen drive for authentication process
			Usage of Laptop for authentication process
		Increased customer faith and attracts new customer	Security in all aspects of network
			Simple and easy way to input
			Time is taken for authentication process
		Efficient memory use, Database is easily manageable	One hash code for comparison and matching
			Cryptographically Encrypted Hash code
			Non reversible Hash code
2	User-friendly issues	Increased customer pool	Quality of multifactor authentication model
			Response time
			Simple method of inputting
			Speed of authentication process
		Reduced Queuing and Reduced waiting process	Good access time
			Simple method of inputting
			Speed of authentication process
		Increased customer satisfaction, retention and acquiring new customers becomes easy	Good Access time
			Good Response time
			Simple method of inputting
			Speed of authentication process
		Increased customer satisfaction,	Automatic process
			Good Access time
			Good Response time
			Simple method of inputting
			Speed of authentication process
3	Input Issues	Ubiquitous authentication with minimum possesition of data	The device used for authentication process
			Availability of network
		Reduced I/O operation	Minimum number of input
			Quality of input
		Increased Customer comfort and satisfaction	Automatic process
			Selection input method
			Good Response time
			Simple method of inputting
			Speed of authentication process
		Reduced parameter requirement for authentication	Multipurpose usability of single input
			Type of input
		Accurate results, error free output	Reliability of the system
			Efficiency of the input
			Quality of input
		Trust and faith over system increases	Increased security
			Increased execution time
			Reliability of the system

			Efficiency of the input
			Type and quality of input
			Security used for protecting input
4	Process Issues	Authentication failure is very rare or practically zero.	Strength of RDBMS
			RDBMS transaction atomicity property
			Ability of the system to handle crashes or failures
		Ensures a safe state at the time of system failure	Strength of RDBMS
			RDBMS transaction consistent property
			Ability of the system to handle crashes or failures
		Enhanced user trust and satisfaction	Strength of RDBMS
			RDBMS transaction atomicity property
			Protected and private authentication process
			Isolation transaction property of DBMS
		Reduced request queue	Availability of authentication system
			Availability of network
			Speed of authentication
		Increased user trust, happiness, and satisfaction	Simple user interface
			Navigational and narrative interface
			Speed of authentication
			Effort free input and process
		Revocability can be done easily if password or Finger-id is compromised	Fast fingerprint-id change option
			Fast password change option
			Hash code representation of fingerprint features and password
5	Performance Evaluation matrix issues	Improved biometric matching and identification rate	The fingerprint image unique feature
			Quality of the fingerprint image
			Ideal false acceptance rate or simply zero.
		Biometric Matching rate and registered user identification can be improved	The fingerprint image unique feature
			Quality of the fingerprint image
			Ideal False Rejection Rate or simply zero
		Biometric Matching rate, registered user, and un-registered user identification error can be improved.	The fingerprint image unique feature
			Quality of fingerprint image
			Ideal Difference between Acceptance and Rejection Rate
		Biometric matching rate, enrol rate failure can be improved	The fingerprint image unique feature
			Quality of the fingerprint image
			The capacity of the system to generate Hash code when partial minutiae details are present in fingerprint image.
		Overall quality of matching can be studied, analyzed, and improved	The fingerprint image unique feature
			Quality of the fingerprint image
			Rejection rate
			Acceptance rate
		Trust and faith over system increases	The structure of the input
			Execution time of the algorithm used (time complexity)
			Over performance of the system

Table-5: Constraints of Multifactor Authentication Model for Verification purpose

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	High Security of the Cloud Drive, USB device, Laptop and Mobile Phone is questionable	Security architecture used in Cloud Drive
			Third party software security architecture used in USB devices
			Password strength used in Laptop

			login process
			Mobile phone pattern lock rigid structure and strength of password
		Good network architecture	Connectivity and security
			Redundancy
			Standardisation
			Disaster recovery
			Growth
		Cryptographically Hash representation of fingerprint image	The fingerprint feature used for Hash code generation
			The strength of Hash code.
			The rate of difficulty for decrypting Hash code.
2	User friendly issues	Requires high configuration system and efficient algorithms	RAM size
			OS and its architecture (32bit 0r 64-bit)
			Processor used
			Single processor/ Multiprocessor
			Clock speed
			Time and space complexity of algorithms used.
		Ability to make difference between registered and un-registered user and Processing power	The features used for identification purpose
			RAM size
			Processor used, Clock speed
			Single processor/ Multiprocessor
			Time and space complexity of algorithms used.
		Dedicated server and network in user-friendly issue	All the features of server required for efficiency
			All the features of network required for efficiency
3	Input Issues	Capacity of the system to differentiate between registered user and intruder with minimum data	The quality of input
			The features used for identification
			All the features of high end configuration system
		Requirement of unique and robust parameter for user Authentication	The quality of input
			The features used for identification
			The salting process used in Hash generation
		User ability to identify correct image	The input selected through selection
			Understandability level of the user
		Operating cost	Cost of the high-end processor
			Cost of the Authentication system
		The ability of the software to make distinction between different context of the same parameter	The feature selected for multipurpose
			The strength of software
			Quality of input
		Quality of the input	Number of minutiae details in fingerprint image
			The correctness of the OTP
			Right password
		Uniqueness, permanence, Universality, and revocability	The features used for generating Hash code
			The database quality to achieve all template protection characteristics
4	Process Issues	Need of good fault tolerance techniques.	Strength of RDBMS

			RDBMS transaction's atomicity, consistency, and isolation property
			The fault tolerance technique used in RDBMS.
			The strength of lock based concurrency control used in RDBMS
		Dedicated server and network	All the features of server required for efficiency
			All the features of network required for efficiency
		Requires navigational and narrative user interface Input should be selective rather than entering	Te explanation displayed in user interface
			Navigational control used in interface
			Input type (selection rather than entering)
5	Performance Evaluation matrix issues	The fingerprint unique property used for identification/Matching	Features used to generate Hash code.
			Quality of Hash code
			The stored Hash code in Database
		Requires good time and space complexity algorithm	The algorithm used for Hash code
			Memory utilized by the algorithm
			Configuration of the system used for authentication

Table-6: Disadvantages of Multifactor Authentication Model for Verification purpose

Sl. No	**Issue**	**Factors affecting**	**Critical Constituent Elements**
1	Security Issues	User level security acceptance by the user	Security architecture used in Cloud Drive, UDB drive, Laptop and mobile.
			Inconvenience in handling these drives
			Security aspect is questionable in third party software
		Network failure	Single point of failure in hardware
			Power problems or issues
			Routing problems
			Human error
		Tampering of data	Un-authorized access to data
			Network failure
		Database failure or server failure	Hardware failure
			File corruption
			File system damage
2	User friendly issues	Hardware and software cost	Cost of RAM
			Cost of Processor
			Cost of the computer system
			OS cost
			Authentication system cost
		Network cost	Bandwidth cost
			Data cost
		High utilization of hardware and software	High utilization of memory and processor
			Space and time complexity
		Complex backend design of interface	To design simple user interface for user

		24 × 7 service	High utilization of processor, and memory
			More power consumption
3	Input Issues	Lack of information	Only fingerprint image are selected
			User personal details are not taken by the system.
		Negligence of the user in selection of input	Lack of concentration of the user
		Misuse of authentication system / More intruder will try to break the system	Continuous availability of the system.
		Significant startup and Maintenance cost	Cost of the high-end processor
			Cost of the Authentication system
		Intruder or un-registered user tries to get multipurpose parameter	Continuous availability of the system.
			Usability of the parameter
		Inability to handle error prone or partial input	Minutiae details are fully missing
4	Process Issues	Requires separate programme for database protection/safeguards	Management of the database
			Essentiality of the Database protection
		Requires lock based concurrency control system	For acquiring isolation property of the database transaction
		Continuous availability of the server increases cost	Requirement of Ubiquitous availability of the server
			Requirement of efficiency of the system
		Complex design of user interface and programme increases cost	Requirement of effort-free authentication process
5	Performance Evaluation matrix issues	Acceptance rate, Rejection rate, Equal error rate, failure to enrol rate, accuracy only used for biometric performance evaluation	Performance evaluation matrices of biometrics data

CONCLUSION

We have studied the Multifactor Authentication Model based on Fingerprint Hash Code, Password, and OTP using ABCD analysis framework. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, (5) Performance Evaluation matrix Issues. The analysis identified the affecting factors for various determinant issues under four constructs advantages, benefits, constraints, and disadvantages. The analysis shows that new model gives good security at network and database level. The Hash code is no reversible and also minimum numbers of input are used for the authentication process.

REFERENCES

1. Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image Authentication. *Journal of Computer Science and Information Technology*, *7*, 195-206.
2. M'raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). *Hotp: An hmac-based one-time password algorithm* (No. RFC 4226).
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.

9. 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.
10. 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.
11. 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.
12. 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.
13. Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.
14. Das, P. P., Chakrabarti, P. P., & Chatterji, B. N. (1987). Distance functions in digital geometry. *Information Sciences*, *42*(2), 113-136.
15. Aithal, P. S., & Aithal, S. (2015). Ideal Technology Concept & its Realization Opportunity using Nanotechnology.
16. Aithal, P. S. (2015). Concept of Ideal Business & Its Realization Using E-Business Model, *International Journal of Science and Research (IJSR)*, 4(3), 1267 - 1274.
17. Aithal, P. S., & Aithal, S. (2016). Impact of On-line Education on Higher Education System. *International Journal of Engineering Research and Modern Education (IJERME)*, *1(*I), 225-235.
18. Aithal, P. S., & Aithal, S. (2015). An Innovative Education Model to realize Ideal Education System. *International Journal of Scientific Research and Management (IJSRM)*, 3(3), 2464-2469.
19. Aithal, P. S., & Aithal, S. (2014). Ideal education system and its realization through online education model using mobile devices. *Proceedings of IISRO Multi Conference 2014, Bangkok*, 140 – 146. ISBN No. 978-81-927104-33-13.
20. Aithal, P. S., (2016). Review on Various Ideal System Models Used to Improve the Characteristics of Practical Systems. *International Journal of Applied and Advanced Scientific Research*, 1(1), 47-56.
21. Aithal, P. S. (2016). The concept of Ideal Strategy & its realization using White Ocean Mixed Strategy, *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 171-179.
22. Acharya, S., & Aithal, P. S. (2016). Concepts of Ideal Electric Energy System for production, distribution and utilization.
23. Aithal, P. S. (2016). Smart Library Model for Future Generations. *International Journal of Engineering Research and Modern Education (IJERME)*, 1(1), 693-703.
24. Aithal, P. S. (2016). Ideal Banking Concept and Characteristics. *International Research Journal of Management, IT and Social Sciences (IRJMIS)*, 3(11), 46-55.
25. Aithal, P. S. (2016). A Comparison of Ideal Banking Model with Mobile Banking System. *International Journal of Current Research and Modern Education (IJCRME)*, 1(2), 206-224.
26. Aithal, P. S., & Pai, T. (2016). Concept of Ideal Software and its Realization Scenarios.
27. Aithal, S., Aithal, P. S., & Bhat, G. (2016). Characteristics of Ideal Optical Limiter and Realization Scenarios Using Nonlinear Organic Materials–A Review.
28. Aithal, P. S., Suresh Kumar P. M. (2017). Ideal Analysis for Decision Making in Critical Situations through Six Thinking Hats Method. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 1-9.
29. Krishna Prasad, K., & Aithal, P. S. (2017). A Customized and Ideal Mobile Banking Technology Using 5G Technology. *International Journal of Management, Technology and Social Science (IJMTS)*, 2(1), 25-37.
30. Aithal, P. S., Shailashree, V. T., Suresh Kumar, P. M. (2015). A New ABCD Technique to Analyze Business Models & Concepts, *International Journal of Management, IT and Engineering (IJMIE)*, 5(4), 409-423.
31. Aithal, P. S. (2016). Study on ABCD Analysis Technique for Business Models, Business strategies, Operating Concepts & Business Systems, *International Journal in Management and Social Science*, 4(1), 98-115.
32. Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy. *International Journal of Applied Research (IJAR)*, 1(10), 331-337.
33. Aithal, P. S., Shailashree, V. T., & Suresh Kumar P. M. (2016). ABCD analysis of Stage Model in Higher Education. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 11-24.
34. Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Analysis of NAAC Accreditation System using ABCD framework. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 30-44.
35. Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Application of ABCD Analysis

Framework on Private University System in India. *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 159-170.

36. Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). The Study of New National Institutional Ranking System using ABCD Framework, *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 389–402.
37. Aithal, S., & Aithal, P. S. (2016). ABCD analysis of Dye doped Polymers for Photonic Applications, IRA-International Journal of Applied Sciences, 4 (3), 358-378.
38. Aithal, P. S., Shailashree, V. T. & Suresh Kumar, P. M. (2016). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 846-858.
39. Shenoy, V., & Aithal, P. S. (2016). ABCD Analysis of On-line Campus Placement Model.
40. Aithal, P. S., Shailashree V. T. & Suresh Kumar P.M. (2016). Factors & Elemental Analysis of Six Thinking Hats Technique using ABCD Framework. *International Journal of Advanced Trends in Engineering and Technology (IJATET)*, 1(1), 85-95.
41. Aithal, P. S. & Suresh Kumar, P. M. (2016). CCE Approach through ABCD Analysis of 'Theory A' on Organizational Performance. *International Journal of Current Research and Modern Education (IJCRME)* 1(1), 169-185.
42. Aithal, P. S. (2017). ABCD Analysis of Recently Announced New Research Indices. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(1), 65-76.
43. Aithal, P. S. (2017). Factor Analysis based on ABCD Framework on Recently Announced New Research Indices, *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 1(1), 82-94.
44. Aithal, P. S. (2017). ABCD Analysis as Research Methodology in Company Case Studies. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 40-54.
45. Aithal, P. S., & Aithal, A. (2017). ABCD Analysis of Task Shifting–an Optimum Alternative Solution to Professional Healthcare Personnel Shortage.
46. Shenoy, V., & Aithal, P. S. (2017). Quantitative ABCD Analysis of IEDRA Model of Placement Determination. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 103-113.