
A Study on Fingerprint Biometric Attendance Maintenance System in Higher Educational Institution Using ABCD Analysis

Krishna Prasad K.

Assistant Professor, College of Computer and Information Science, Srinivas University,
Mangaluru-575001, Karnataka, India
E-mail: karanikrishna@gmail.com

Abstract

The drastic developments in Information and Communication Technology enabled many types of technology-aided attendance maintenance system in Higher Educational Institutions. A fingerprint is one of the most common and popularly known biometric systems all over the world. The usage of fingerprints for authentication is a universally prevalent solution and a majority of the population has legible fingerprints. This is more than a number of humans who have passports, license and identification cards. It has fairly one of the maximum accurate forms of biometrics available. Fingerprint biometric has been utilized in numerous areas together with entry management and door-lock control, smart cards, vehicle ignition control framework and fingerprint controlled access control system. Because the superior technology allows even extra compact fingerprint sensor size, the variety of application is expanded to the cellular market. One of the important applications of the biometric system is in attendance maintenance and which is incorporated in many of the higher educational institutions. From olden days, three styles of fingerprints may be obtained, namely, exemplar prints, latent prints and plastic prints. In this paper, we study fingerprint attendance maintenance system with its advantages, benefits, constraints, and disadvantages. We use focus group interaction method to gather information of fingerprint biometric attendance system. This paper also discusses some recommendations for fingerprint biometric attendance system. This paper could play an active and supportive role in fingerprint biometric attendance based researches.

Keywords: *Fingerprint Biometric, Higher Educational Institution, latent prints, ABCD Model, Fingerprint biometric-based attendance system.*

INTRODUCTION

A fingerprint is an influence or lines of an impression from the friction ridges, from the floor of a fingertip of a person's finger. A friction ridge is a raised part of the epidermis on the fingers and includes one or extra linked ridge units of friction ridge skin. These are every so often regarded as "epidermal ridges", which might be because of the underlying interface between the dermal papillae of the dermis and the inter-papillary of the epidermis. Those epidermal ridges serve to enlarge the vibrations brought on, for example, at the same time as fingertips brush across a choppy floor, higher transmitting the alerts to sensory nerves concerned in nice texture perception [1]. Those ridges additionally assist in gripping rough surfaces, as well as clean wet surfaces. Impressions of fingerprints may be left behind on a floor with the aid of the herbal secretions of sweat from the eccrine glands which can be present in friction ridge pores and skin, or they will be made via ink or other materials transferred from the peaks of friction ridges at the pores and skin to a pretty easy floor including a fingerprint card [2]. Fingerprint statistics commonly incorporate impressions from the pad at the remaining joint of fingers and thumbs, although fingerprint cards also commonly record portions of lower joint areas of the hands. The basic standards of fingerprint generation were scientifically mounted by Sir Francis Galton, a British scientist referred as the father of fingerprint technological advances and are given below.

Permanency or Persistence: This first fundamental principle of fingerprints describes their area of expertise. In keeping with this principle, a fingerprint is a human being feature and no two fingers are observed to have identical ridge styles.

Consistent and Constant: This essential property states that a fingerprint, all through the lifetime of an individual, remains unchanged. They may extend with bodily growth, but the patterns remain equal. This is the most generous characteristic of fingerprints that make them useful for identity management, authentication, and biometric packages. Even the signature of someone, that's taken into consideration a behavioral biometric, may change beyond regular time, but fingerprints remain unchanged throughout someone's lifetime. Fingerprints by no means change themselves however in some cases, because of wound or harm (as an example, excessive burn or working in positive industries) they will distort or disappear. Being on fingertips, they have usually the first point of physical contact, but, they are no longer broken via superficial injuries. A few clinical conditions also can purpose fingerprints to vanish.

Uniqueness: Two person fingerprints at the outset might look similar, but every person fingerprint ridge patterns are unique. These ridge patterns can be used for systematic classification in diverse applications.

Fingerprint biometric has been utilized in numerous areas together with entrance management and door-lock programs, smart cards, vehicle ignition control framework and fingerprint controlled access control system. Because the superior technology allows even extra compact fingerprint sensor size, the variety of application is expanded to the cellular market. Thinking about the developing segment of the existing mobile marketplace, its ability is the best of all utility markets. The fingerprint is one of the most frequent and most

dependable assets utilized in criminology to pick out criminals and fraudulent persons. It is also used within the identification of unidentified body wherein fingerprint facts are compared with current databases. They may be an increasing number of users in many crucial carrier oriented industries like banking, licensing and passport, in which usage of fingerprint reduce the incidence of forgery, impersonation, and frauds to a brilliant volume. They have utilized in assets and civil instances in which the usage of historical records of the registration department and on files allows to solve important cases.

Fingerprint attendance system purpose is to automate the manual attendance management system using unique properties of fingerprint technology [3]. In order to identify the employee and to know their entering an institution and leaving the institution can efficiently capture and processed using optical or ultrasonic or any other type of sensors. Almost many higher education institutions are using today fingerprint biometric attendance system to maintain organization employees in and out time [4-18].

In this paper, we study the fingerprint attendance maintenance system with its advantages, benefits, constraints, and disadvantages. We use focus group interaction method to gather information on fingerprint biometric attendance system. This paper also discusses some recommendations for fingerprint biometric attendance system. This paper also discusses some recommendations for fingerprint biometric attendance system. The Paper is structured under different sections. The First section discusses the introductory theory of fingerprint technology. Section Two investigates a related area of research or discussion of already done research in this area. Section Three describes the problem and Objectives of this research study. Section Four describes ABCD analysis framework. Section Five narrates about ABCD analysis of Fingerprint biometric attendance system. Section Six describes some recommendation for fingerprint biometric attendance system based on the existing study. Section Six concludes the papers.

2. RELATED RESEARCH

In the literature there are many research papers are available for attendance management system using an automated system which includes different biometrics like face, Iris, Fingerprint, Voice or Speech, gait behaviour and many more. But in this paper, the only fingerprint based attendance management system only considered as related area research. Taxila, P. (2009) [19] proposed a fingerprint-based attendance management system for an educational institution which had one fingerprint sensor and LCD screen placed at every classroom door. This facility can be used by students in order to enter their attendance. A dedicated server is maintained for attendance purpose and every time when a student places his/ her fingerprint on the sensor it identifies the particular student and attendance is updated on the server. The system is found to reduce the burden of manual work and also saved the time. Mishra, R., & Trivedi, P. (2011) [20] proposed a framework using which student attendance maintenance system automated and kept online. They found that the student identification and attendance management using their fingerprint is faster compared to any other ordinary fingerprint identification system. Their identification system was compared

with n2 matching based identification system and new system took only 0.0157 seconds for matching, while counterpart system took 0.1994 seconds in worst case scenario of about 150 sizes of students. Chen, H. et al. (2002) [21] proposed an intelligence entrance guard system, based on fingerprint identification system. In this paper, they have addressed challenges of earlier authors or research problems and came up with some solution for efficient identification of user using the special techniques of intelligence system and fingerprint identification system. Chandramohan, J. et al. (2017) [22] used minutiae-based fingerprint recognition or identification system for student attendance or for college administration with the aid of GSM. The attendance maintenance system uses fingerprint sensor along with face recognition module used also for the purpose of identifying a missing person with the help GSM. Rao, S., & Satoa, K. J. (2013) [23] proposed employee or student attendance maintenance system with an intention to make the system simple, fast, accurate and very efficient. The study was conducted in this paper based on the quantitative method of data collection, which is using questionnaires based on fingerprint matching technologies. Zainal, N. I., et al. (2014) [24] designed and developed a portable automated attendance maintenance system. In this Model independent source of energy was mainly operated and its miniature design made the system highly secured and optimal. The new portable fingerprint based attendance maintenance system addressed the weakness or flaws of existing manual attendance system.

3. PROBLEM STATEMENT AND OBJECTIVE OF THE STUDY

A finger manual attendance system generally paper is used for maintaining and keeping track of attendance of students or employees in the higher educational institution. The manual method usually requires paper and many other stationary materials, which is difficult to change if required to maintain neatness. There are many works carried out for keeping track of attendance using different types of biometric recognition devices or through automated software programs. Some software is created for attendance maintenance but which requires user intervention as some entries to register attendances. In higher educational institutions these users are usually students or employees of the institution. There is many attendances tracking system like through face recognition, which requires high expensive hardware and software supports. This study concentrates mainly on fingerprint based attendance maintenance system. The main objective of this study is

- Ø To understand and know the research work carried on fingerprint biometric-based attendance maintenance system
- Ø To analyze the fingerprint biometric attendance maintenance system using ABCD analysis by considering various determinant issues and critical constituent element
- Ø To propose some recommendations based on ABCD analysis.

4. ABOUT ABCD ANALYSIS

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 given surroundings may be studied the usage of SWOT analysis, SWOC evaluation, PEST analysis, McKinsey's framework, ICDT version, Porter's 5 force model and so on. Recently a new model is introduced to these analysis areas called ABCD analysis framework 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 the ABCD framework can be used to assign an 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 a new system or new strategy or new generation or a 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. ABCD analysis framework can be used for analyzing private universities (Aithal et al., 2016b), New National Institutional Ranking System Dye-doped Polymers for Photonic Applications, Annual research productivity and Online Campus Placement Model and also many more [25-33].

5. ABCD ANALYSIS OF FINGERPRINT BIOMETRIC ATTENDANCE MAINTENANCE SYSTEM

Fingerprint Biometric Attendance System used in this research work can be analyzed using ABCD Analysis. The complete framework is divided into various issues, the area which new system is focused. Various key properties and affecting the area of the new system may be identified and analyzed in 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 6.1. 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 Fingerprint Biometric Attendance System are: (1) Security issues, (2) Ease of use Issues, (3) Input issues, (4) Process issues, (5) Performance Evaluation matrix issue

(1) Security Issues: Security is very important in the Fingerprint Biometric Attendance System. 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 Fingerprint Biometric Attendance System, security refers safeguarding the user personal data used for attendance process, and proxy attendance should be avoided or rejected by the system. The affecting factors of Security issues include a Fingerprint image, 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) Ease of Use Issue: The Ease of Use of Fingerprint Biometric Attendance System 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 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 the 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: This 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 properties 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 issue under four constructs are derived by a qualitative data collection instrument namely, focus group method and are listed in Table 2.

Table 1: Analysis of Fingerprint Biometric Attendance Maintenance System

Determinant Issues	Key properties	Advantages	Benefits	Constraints	Disadvantages
Security Issues	User-level security (For Biometric Image)	Easy to secure using sensors	increases demand for different types of fingerprint sensors	Security and performance of sensors	Acceptance by the user
	Database or Template Security	Single compressed image	Efficient memory use,	Database capacity to handle image	Database failure, Server failure

		occupies less space	Database is easily manageable	efficiently	
Ease of user Issues	Response time	More user s can register their attendance with minimum time	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 hardware and software resources are too high complex backend design of the user interface
	Availability	Ubiquitous attendance maintenance	Reduced request queue	Dedicated server and network	24 × 7 working server
Input	Minimum	minimum	User get	Capacity of	Lack of

Issues	Possession	knowledge parameters required for authentication	authenticate anywhere without carrying anything	the system to differentiate between registered user and intruder with minimum data	information
	Least 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 input	Ubiquitous Authentication process	Increased user satisfaction	Requirement for high configuration system and network availability	Misuse of 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 a distinction between the 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	Quality of the input	Inability to handle error prone or partial

			output		input
	Security	User personal data protection	Trust and faith over system increases	Uniqueness, permanence, Universality, and revocability	Cost of the system become high.
	Execution time	Increased growth rate in authentication	Trust and faith over system increases	Requires a 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 on failure is very rare or practically zero.	Need of good fault tolerance techniques.	Requires separate programme for database protection /safeguards
	Consistency	Ensures the consistent state at the time of system failure	Authentication on 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 of 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 entering	Complex design of user interface and programme increases cost

Performance Evaluation matrix issues	False acceptance rate	Ability of the system to differentiate registered and unregistered user can be tested.	Improved biometric matching and identification rate	The fingerprint unique property	Not useful to identify 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	Overall quality of matching can be studied,	Sophisticated filtering, feature enhancement techniques	Not useful to identify performance of non-biometric factors

		studied	analyzed, and improved	are essential Good false rejection and acceptance rate are compulsory	
	Execution time	The rate of users get authenticated increases per unit time.	Trust and faith over system increases	Requires a good time and space complexity algorithm	Requirement of Good configuration system increases cost

5.1 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 ABCD model and tabulated in Tables 2 to 5.

Table 6.2: Advantages of Fingerprint Biometric Attendance Maintenance System

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	Mobile/Smart Phone	Structure of locking pattern
			Password strength
		Laptop	Password strength
		Sensor capacity in unique identification	Type of sensor used.
2	Ease of use issues	Increased rate of growth of attendance process	Type of the algorithm used
			Conversion time required to convert fingerprint image to identifiable format
			Time required for fetching training and test data
		Increased attendance request per unit time	Speed of Matching function
			Ability of concurrent attendance entry
		Minimum prior information of the system required	Efficiency of training and test code matching rate
			The ability of the system to enter attendance without prompting anything or with minimum input (only fingerprint image)
		Ubiquitous attendance entry in ease of use issue	The system used for attendance process
			Availability of network

3	Input Issue	Minimum Knowledge parameters	The ability of the system to authenticate without prompting or without accepting more input from the user.
		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 attendance process in input	The device used for attendance entry 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			
4	Process Issues	Attendance 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 attendance process
			Availability of network
		User freely and easily interacts with attendance process system	Simple user interface
			Navigational and narrative interface
5	Performance Evaluation matrix issues	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

		Ability of system to identify registered user can be improved	The fingerprint image unique feature
			Quality of the fingerprint image
			False Rejection Rate
		Ability of attendance maintenance system to identify rejection and acceptance rate can be easily studied	The fingerprint image unique feature
			Quality of fingerprint image
			Difference of Acceptance and Rejection Rate
		The overall matching performance and accuracy can be easily studied	The fingerprint image unique feature
		Increased growth rate in attendance process due to performance issue	Quality of the fingerprint image
			Rejection rate
			Acceptance rate
			The structure of the input
			Execution time of the algorithm used (time complexity)

Table 6.3: Benefits of Fingerprint Biometric Attendance Maintenance System

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	Increases demand for Sensors	Usage of mobile sensors attendance entry process
		Increased customer faith and attracts new customer	Security in all aspects of network
			Simple and easy way to input
		Efficient memory use, Database is easily manageable	Time taken for attendance entry process
			Compressed image
2	Ease of use issues	Increased customer pool	Quality of attendance maintenance model
			Response time
			Simple method of inputting
			Speed of attendance entry process
		Reduced Queuing and Reduced waiting process	Good access time
			Simple method of inputting

		Increased customer satisfaction, retention and acquiring new customers becomes easy	Speed of attendance process
			Good Access time
			Good Response time
			Simple method of inputting
			Speed of attendance process
		Increased customer satisfaction,	Automatic process
			Good Access time
			Good Response time
			Simple method of inputting
			Speed of attendance process
3	Input Issue	Ubiquitous authentication with minimum possession of data	The software used for attendance maintenance 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 attendance 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	Attendance entry failure is very rare.	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

		Enhanced user trust and satisfaction	Ability of the system to handle crashes or failures
			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
5	Performance Evaluation matrix issues	Improved training and test data matching and identification rate	The fingerprint image unique feature
			Quality of the fingerprint image
		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, enroll 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

		Trust and faith over system increases	Rejection rate
			Acceptance rate
			The structure of the input
			Execution time of the algorithm used (time complexity)
			Over performance of the system

Table 6.4: Constraints of Fingerprint Biometric Attendance Maintenance System

Sr. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	High Security sensor, Laptop and Mobile Phone is questionable	Security architecture used in sensors and in system
			Password strength used in Laptop login process
			Mobile phone pattern lock rigid structure and strength of password
		Good network architecture	Connectivity and security
			Redundancy
			Standardization
			Disaster recovery
			Growth
2	Ease of use issues	Requires high configuration system and efficient algorithms	RAM size
			OS and its architecture (32bit Or 64-bit)
			Processor used
			Single processor/ Multiprocessor
			Clock speed
			Time and space complexity of algorithms used.
		Ability to make difference between registered and unregistered 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 ease of use issue When implemented through	All the features of server required for efficiency
			All the features of network

		client/server model	required for efficiency
3	Input Issue	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 attendance process	The quality of input
			The features used for identification
		Operating cost	Cost of the high-end processor
			Cost of the Attendance maintenance 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
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	The fingerprint unique property used for	Features used to generate Hash code.

	matrix issues	identification/Matching	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 attendance entry process.

Table 6.5: Disadvantages of Fingerprint Biometric Attendance Maintenance System

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	User-level security acceptance by the user	Security architecture used in attendance maintenance system, 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
2	Ease of use 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 services	High utilization of processor, and memory More power consumption
3	Input Issue	Lack of information	Only fingerprint image are selected User personal details are not taken by the system.
		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 enroll rate, accuracy only used for biometric performance evaluation	Performance evaluation matrices of biometric data

6. RECOMMENDATION OF THE STUDY

Based on the Fingerprint Biometric attendance Maintenance System-ABCD analysis some recommendations are made in this study, which is as follows.

- Ø Using High capacity and a powerful sensor for fingerprint capturing improves the accuracy rate.
- Ø Always store fingerprint image data in Hash or nonrevocable format.
- Ø Reduce the amount of memory occupied by the training and test image by converting it to the Hash form.
- Ø Use high efficiency and robust algorithm to match sample or test fingerprint image with training dataset or template.
- Ø Changes in finger depending on weather condition or a cut or wound in finger does not affect the system performance in this model.
- Ø Security details database table consist of only two fields as Fingerprint Hash-id and double folded encrypted password.

7. CONCLUSION

The fingerprint is very not unusual and popular biometric of type traits due to its universality, distinctiveness, and permanence and additionally, many advances and new researchers are to be had in this discipline. Fingerprint identification technology era has various blessings for much less price and non-invasive manner of acquisition and therefore is one of the maximum frequently used mechanisms.

This paper discussed the Fingerprint Biometric Maintenance System with its advantages, benefits, constraints, and disadvantages. 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 Fingerprint Biometric Attendance System are (1) Security issues, (2) Ease of use Issues, (3) Input issues, (4) Process issues, (5) Performance Evaluation matrix issue. This paper also discussed some recommendations for fingerprint biometric attendance system. This paper could play an active and supportive role in fingerprint biometric attendance based researches.

REFERENCES

- [1] Kwok, R. (2009) Fake finger reveals the secrets of touch, *Nature*, Vol. 29, <http://www.nature.com/news/2009/090129/full/news.2009.68.html>, Last Access Date: 14-08-2017.
- [2] Olsen, R. D. (1972). The chemical composition of palmar sweat. *Fingerprint and Identification Magazine*, 53(10), 3.
- [3] Basheer, K. M., & Raghu, C. V. (2012, December). Fingerprint attendance system for classroom needs. In *India Conference (INDICON), 2012 Annual IEEE* (pp. 433-438). IEEE.
- [4] 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>
- [5] 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>
- [6] 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>
- [7] 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>
- [8] 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>

[9] 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>.

[10] 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>

[11] 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>

[12] 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: <http://dx.doi.org/10.5281/zenodo.1602012001>

[13] 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>.

[14] 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>.

[15] 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>

[16] 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://dx.doi.org/10.21276/sjeat.2018.3.1.3>

[17] 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://dx.doi.org/10.21276/sjbms.2018.3.1.10>

[18] 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>

[19] Taxila, P. (2009). Development of academic attendance monitoring system using fingerprint identification. *IJCSNS*, 9(5), 164.

[20] Mishra, R., & Trivedi, P. (2011). *Student Attendance System Based on Fingerprint Recognition and One to Many Matching* (Doctoral dissertation).

[21] Chen, H., Zhang, X., & Tong, T. (2002). An Intelligent Card Entrance Guard System Based on Fingerprint [J]. *Computer Engineering*, 7, 080.

[22] Chandramohan, J., Nagarajan, R., Dineshkumar, T., Kannan, G., & Prakash, R. (2017). Attendance Monitoring System of Students Based on Biometric and GPS Tracking System. *International Journal of Advanced engineering, Management and Science*, 3(3).

[23] Rao, S., & Satoa, K. J. (2013). An attendance monitoring system using biometrics authentication. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(4).

[24] Zainal, N. I., Sidek, K. A., Gunawan, T. S., Manser, H., & Kartiwi, M. (2014, November). Design and development of portable classroom attendance system based on Arduino and fingerprint Biometric. In *Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on* (pp. 1-4). IEEE.

[25] 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*, 5 (4), 409 – 423.

[26] 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. DOI: <http://doi.org/10.5281/zenodo.161137>.

[27] Aithal, P. S. and Pai T, Vaikunta (2016). Concept of Ideal Software and Its Realization Scenarios. *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 826-837.

[28] Aithal, P. S., Shailashree, V. T. & Suresh Kumar, P. M., (2016d). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 846-858. DOI: <http://doi.org/10.5281/zenodo.62022>.

[29] Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2015). A New ABCD Technique to Analyze Business Models & Concepts.

[30] Aithal, P. S., Shailashree, V. T., & Suresh Kumar P. M., (2016a). ABCD analysis of Stage Model in Higher Education. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 11-24. DOI: <http://doi.org/10.5281/zenodo.154233>.

-
- [31] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016b). Application of ABCD Analysis Framework on Private University System in India. *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 159-170. DOI: <http://doi.org/10.5281/zenodo.161111>.
- [32] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016c). The Study of New National Institutional Ranking System using ABCD Framework, *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 389–402. DOI: <http://doi.org/10.5281/zenodo.161077>.
- [33] 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. DOI: <http://dx.doi.org/10.21013/j.as.v4.n3.p1>.