Blockchain Technology in Biometric Database System

Conference Paper · November 2022

DOI: 10.1109/ICCAKM54721.2022.9990133

5 authors, including:

Rajesh Kumar D
symbiosis International (Deemed University)
134 PUBLICATIONS **1,077** CITATIONS
SEE PROFILE

Md. Akkas Ali
Bangabandhu Sheikh Mujibur Rahman Science and Technology University, Gopal…
22 PUBLICATIONS **86** CITATIONS
SEE PROFILE

Balamurugan Balamurugan
VIT University
217 PUBLICATIONS **2,329** CITATIONS
SEE PROFILE

Vandana Sharma
CHRIST University Delhi NCR Campus India
48 PUBLICATIONS **204** CITATIONS
SEE PROFILE

2022 3rd International Conference on Computation, Automation and Knowledge Management (ICCAKM) | 978-1-6654-5319-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCAKM54721.2022.9990133

Blockchain Technology in Biometric Database System

Anamika Singh
PhD Scholar, School of Computing Science and Engineering
Galgotias University
Greater Noida, U.P, India
anamika.21scse3020003@galgotiasuniversity.edu.in

Dr. Rajesh Kumar Dhanaraj
School of Computing Science and Engineering
Galgotias University
Greater Noida, U.P, India
sangeraje@gmail.com

Md. Akkas Ali
PhD Scholar, School of ComputingScience and Engineering Galgotias University
Greater Noida, U.P, India
md.21scse3010038@galgotiasuniversity.edu.in

Dr. Balamurugan Balusamy
Associate Dean Student
Shiv Nadar University
Noida, U.P, India
kadavulai@gmail.com

Dr Vandana Sharma
Amity Institute of Information Technology
Amity University
Noida Campus, U.P, India
vandana.juyal@gmail.com

Abstract— **The Biometric system can be understood as a system that deals with an automated recognition of individual based on their physiological aspects (face, fingerprints, iris, retina) and behavioral patterns (signature, posture etc.). Biometric system works on feature extraction and feature matching. The feature is extracted in the form of fingerprints, iris and retina and then it is matched by the information stored by measuring the same patterns of particular individual, this process is feature matching. Between the two, works template database which is a central point from where every time the feature extracted is matched for confirming the identity of a person.. If the database is breached by the hacker, then the data could be used for falsifying the identity of the person. The paper focuses to implement blockchain technology in a biometric system in a manner that every record of individual is maintained using a blockchain so that it can't be hampered by the hacker. Blockchain works as adecentralized repository of data which we assume to be the most suitable approach to hold the credentials of individuals and thus avoiding an unauthorized access to the systems. Making changes to blockchain is a complex and time-consuming task for any unwanted user. Many researchers contributed their work highlighting the security issues of the biometric system when applied practically. They noted that the fingerprint of an individual remains the same over life and once applied can't be modified when compares with non- biometric systems which makes use of passwords and if forgotten or breached could be changed. Some of them conveyed that the biometric system is safe when only considering its physical implementation but the database created is still under threat.**

Keywords— Biometric system, blockchain technology, consensus algorithm, encryption algorithm, decryption algorithm

I. Introduction

Biometrics' origin is from a Greek word "bios" implies life and "metrics" which means measure. As whole biometrics can be explained as a logical evaluation of biological attributes. If we go back to the 14th century, then China was the first to take fingerprints of its trader and their families to distinguish them from all others. Fingerprinting originated from then on, so one could argue that biometric systems are not new to the world of technology [1]. Later in the 19th century, the scientist Alphonse Bertillon discovered a system that takes measurements (of photos and recorded lengths, height of one foot, hand and toe) of the human bodyto determine. But this approach was later disapproved as it was claimed that the person with same body measurement falsely taken as one. Biometric works with two phases:

- Registration Phase
- Matching Phase

The registration phase collects the data from source as the installed step then processes the signals, after completing signal processing it extracts the feature as whether it is fingerprint, face recognition etc and registers the same. In the second phase that is the matching phase it takes biometric feature as input which was previously registered in the registration phase, matches the two and make a check that if both the biometric data matches or not, if found same then the authentication is succeeded else announced failed or rejected. The proposed paper focuses on creating and maintaining the template database using blockchain.. The benefits provided by blockchain technology are summarized in "Fig. 2" [2].

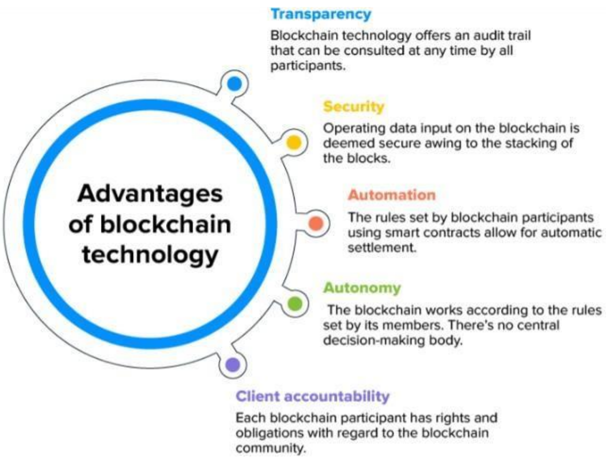

Advantages of blockchain technology
Transparency
Blockchain technology offers an audit trail that can be consulted at any time by all participants.
Security
Operating data input on the blockchain is deemed secure awing to the stacking of the blocks.
Automation
The rules set by blockchain participants using smart contracts allow for automatic settlement.
Autonomy
The blockchain works according to the rules set by its members. There's no central decision-making body.
Client accountability
Each blockchain participant has rights and obligations with regard to the blockchain community.

Fig. 2. Benefits provided by blockchain technology

The blockchain plays a vital role in terms of:

- Transparency: This means the data stored in the blockchain is available to all the participants at any time.
- Security: The information in the blocks of the blockchain is highly secure as the modifications can't be carried out easily.
- Automation: It allows automatic settlement by the rules marked by the participants of the blockchain.
- Autonomy: There is the absence of any central decision-making body, the blockchain is governed by the rules set by the members of the blockchain.
- Client accountability: Every blockchain participant has rights and obligations with respect to the blockchain community.

A. *History of biometric system*

True biometric systems began to evolve in the latter of 20th century.The journey of biometric system gone through a long way.

TABLE I. TIMELINE OF BIOMETRIC HISTORY [2]

Year	Biometric system	Description
1858	Hand Image	First systematic capture of hand images for identification is recorded
1883	Fingerprint	The use and process were given
1870	Anthropometric	Development of anthropometrics for individual identification.
1892, 1896	Fingerprint	A classification system was developed and its use began
1936	Iris pattern	The concept of iris pattern is proposed
The 1960s	Face recognition and speech production	The form became semi-automated and the first model for acoustic speech production is created
1965	Signature recognition	The research for this system began
1969	Fingerprint	FBI pushes to make fingerprint recognition an automated process
The 1970s	Face recognition and speech recognition	This concept takes another step towards automation and also the behavioral components of speech recognition are modelled
1974	Hand Geometry	First commercial systems for hand geometry become available.
1988	Face recognition	First semi-automated facial the recognition system is deployed
1994	Palm recognition	The system is benchmarked and first iris recognition algorithm is patented
2000	Face recognition	The first face recognition vendor test is held
1988	Face recognition	First semi-automated facial the recognition system is deployed

Fig. 4. Timeline of Biometric History

II. RELATED WORKS

In the paper [3], the authors have done the database management system for agricultural system. The authors of the paper [4] implemented the database management system for prevention of crypto-ransomware. The biometric based recognition system database is developed by [5]. The authors have done the database management system for biometric system [6]. In paper [7], The authors maintained a database system for proof of Elapsed Time Consensus. The authors of the paper [8] done the database management systems for DNA and Fingerprint data. A MySQL database are managed for fingerprint data by the authors of the paper [9]. A database management system for DNA and Fingerprint based identification system is designed by [10]. The database management system for event participants authentication by using face recognition data are developed by the authors of the paper [11]. For the students and employees of an academic institute, smart attendance and leave management system by using fingerprint recognition are done by [12]. The authors of the paper [13] have done DNA and Fingerprint based database management system. A somewhat reduced fingerprint template was given privacy protection by [14]. In the study, the thinning enrollment fingerprint image and fingerprint template kept in an online database for authentication conceal the user's identity. They asserted that with such a system, it would be nearly hard for an attacker to steal a template from a stolen online template database and reveal the user's identity [15]. In [16] proposed a technique of cryptography that employs arbitrary integers as the private key for image calculation and an image as the public key. To conceal biometric data [17] suggested using steganography a set of photos of faces with data i. e. fingerprint minutes on them. The purpose of this is to communicate data. The concealable biometric approach was suggested by [18] as a way to secure the template database. The system alerts the database administrator that there is a problem with the biometric template in the database in the event that a forger attempted to change or alter it [19]. String permutation was suggested by [20] as a method for protecting template databases. After establishing a handy template, biometric data is encrypted and discarded. On a random reference table drawing, [21] suggested a secret-protective Cancellable Iris Pattern Encoding and New Cancellable Iris template. The Biometric attendance management system is designed by the authors of the paper [22] and the work conveyed and compares some basic properties of different biometric systems and listed them in a table II. The paper explains a approach of cancelable finger-vein, bio-cryptosystembased on smart cards allows to encode the healthcare credentials and ensuring safety to the indigenous information on a biometrics system.

TABLE II. PROPERTIES OF DIFFERENT BIOMETRIC SYSTEMS

Characteristics	Face	Fingerpr int	Speech	Hand	Iris	Signa-ture
Ease of use	M/H	H	H	H	L/M	H
Accuracy	M	H	M	M	H	M/L
Acceptability	H	M	H	M/H	L/M	H
Security	M	H	M	M	H	M/L
Permanence	M	H	M/L	M/H	H	M/L

Fig. 5. Properties of different biometric system

Where L= low, M= medium, L=large. In his study focused on hoe different biometric systems work, and a comparative study is made between the most commonly used six biometric techniques based on the following characteristic parameters: ease of use, the accuracy offered, acceptability of particular system, the most concerned its security and the permanence are summarized in the table. The most complex system to use is the iris recognition as compared to others. Accuracy offered by all the six systems is appreciable leaving signature-based systems, the least acceptable system is the iris recognition and in terms of security provided, except signature-based system, all five are the secure systems and the permanence of iris recognition and signature-based systems are not commendable. . (Shaykh Siddique, 2021) made a comparison between the biometric systems and the pin/password pattern to know the most preferable system as shown in “Fig. 4” [23].

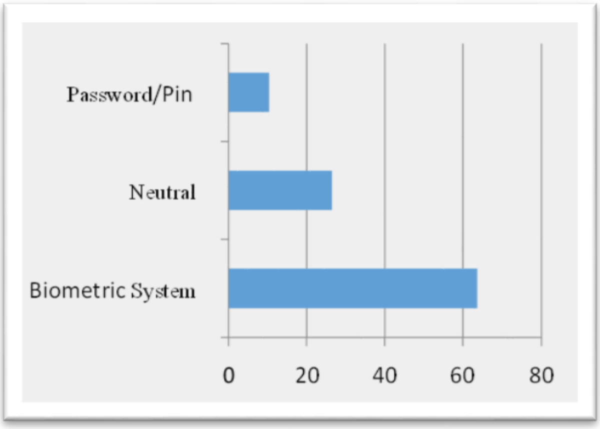


Fig. 6. Password/Pin Vs Biometrics

In Bangladesh, 63.63% hold the opinion that the biometric systems are more secure than the password or pin-based system, 10.32% completely disagreed from the thought that the systems are safe and 26.45% population didn’t provide any response to the question. The study is followed by conducting a survey to know the issues faced by the population and are summarized further in “Fig. 5” [23].

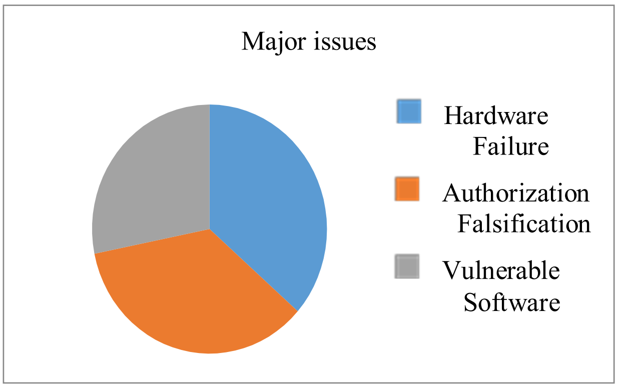


Fig. 5. Major issues of Biometric

The participants who found the biometric systems unsafe figured out what are the issues they face in biometrics systems. The study noted that 66% among the total participants faced the problem of hardware failure. One of the major issues was falsifying authorization and identification of a real person and the count for this issue was 64% and the issues related to unsafe recording of one’s identification information scored 51% from the participants. Studies conducted further focused on the material and methods that were installed as asecurity tool to make a biometrics system private. The proposed tools suggested by the studies are Jinja2, Short Message Service (SMS), an encryption and the decryption algorithm [24].The functioning of an encryption and the decryption algorithm are elaborated as:

A. Encryption Algorithm

Step 1: The user is required to enter the username and the password held with him as his log in credentials.

Step 2: The same is checked from the database where the valid username and password is stored that is held by authorized user

- If the check made is correct, an authentication code is passed to the user

- If check is wrong, user is guided to login again

Step 3: After receiving the AC the user is asked to enter the same and then it is again checked with the AC in the database that is provided to the use

Step 4: If the input data is matched.

- Two Fernet keys are generated which are then integrated to form a single Multi Fernet key.
- The Multi Fernet key is then combined with the biometric information that was registered and stored.
- The next step is to convert this biometric data into biometric template (byte file and text file) by making use of encryption algorithm.

Step 5: If the input data is still not matched, again the user is advised to check and enter the valid username and password.

B. Decryption Algorithm

Decryption the process of converting or decoding the cypher or decoded text or data to the original or plain text

1) Algorithm:

Step 1: The admin is required to enter the username andpassword.

Step 2: The same is checked from the database where the validusername and password is stored that is held by authorized user.

- If the check made is correct, an authentication codeis passed to the admin.
- If check is wrong, admin is asked to login again.

Step 3: After receiving the AC the admin is requested to enterthe same and then it is again checked with the AC in thedatabase that is provided to the user.

Step 4: If the input data is matched.

- Two Fernet keys are generated which are then integrated to form a single Multi Fernet key.
- The Multi Fernet key is then combined with the decoded biometric template which includes the bytefile and the text file.
- With the help of decryption algorithm this biometric template is then converted into the

original or plain text (biometric data).

Step 5: If the input data is still not matched, again the admin is advised to check and enter the valid username and password.

TABLE III. LEVEL OF VULNERABILITY

Blockchain	Subgroup-Finding algorithm (Shor’s)	Amplitude Amplification (Grover’s)
Bitcoin	×	–
Ethereum	×	–
Litecoin	×	–
Monero	×	✓
ZCash	×	–

Fig. 8. Level of vulnerability

Where × indicates blockchain has strong level of vulnerability against attacks, - denotes medium level of vulnerability and ✓ assumes that cryptocurrency is currently safe from quantum attacks

III. PROPOSED FRAMEWORK

In this section of the paper, the proposed framework is described through the algorithm that guides the use of blockchain technology in storing and maintaining the identification information of an individual. The steps of the algorithm are discussed below:

i. A single record is maintained and recorded at a single block of the blockchain construction.

ii. The hash is generated for the block to distinguish the blocks from one another and thus maintaining the non- redundancy of data.

iii. With every new block, there has to be the previoushash which is the hash of the previous block.

iv. As the new record enters, again the block is generated using different algorithms and a hash is created.

v. When one wants to alter even a single piece of information from the block, then needs to follow certain steps:

- Foremost step is to ask from every authority in the network holding a copy of the associated blockchainstructure.
- The voting takes place where every person in the network votes whether the change has to be made ornot. This process or rule of voting is known as Consensus Rule.
- The results from the voting are then examined and the action has to be taken based on the majority votes.
- If the majority says Yes, the data will be altered elsethe change is considered irrelevant.

vi. Each time the person uses the biometric system, at the same moment the system will take to the block of the same individual’s record that was stored beforehand and that is compared to the “Smart Contract Block” generated using the encryption andthe decryption algorithm discussed above. When match founds to be the same, then only allow the one to proceed. And if not matched, gives an error and isnot allowed to proceed.

These steps work continuously in the blockchain structure to control the data breach, enhancing and assuring the integrity, security and availability of data for future purposes

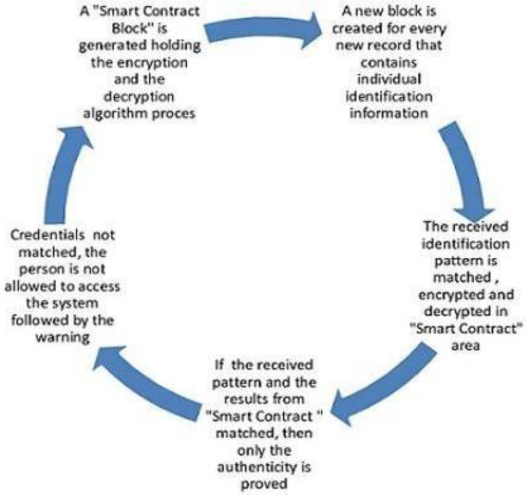

A "Smart Contract Block" is generated holding the encryption and the decryption algorithm proces
A new block is created for every new record that contains individual identification information
The received identification pattern is matched , encrypted and decrypted in "Smart Contract" area
If the received pattern and the results from "Smart Contract " matched, then only the authenticity is proved
Credentials not matched, the person is not allowed to access the system followed by the warning

Fig. 9. Proposed Framework

IV. FINDINGS AND CONTRIBUTION

With the proposed paper, a methodology is adopted to contribute the security and privacy of individual’s credentials and personal information. Passports/ pan cards and other such identity prove cards use the technology of biometric to keep safe the personal information of a person which if stolen and revealed results into unexpected trouble. So, the paper focused to create and maintain the backend or the database containing all the personal records of the individual using blockchain technology. As in today’s world a user can’t blindly trust thethird party as how, when and why they are falsifying one’s identity. Blockchain technology assures the security of one’scredentials as without gaining authority and permission fromall the authorized people no one can alter a single block. So, the database maintained for biometric will be safe and can’t be hacked and hampered easily and the personal records will not be used for any falsification purposes. With this approach, the stated work islooking forward to enhance the security and integrity and to assure the availability of one’s personal identification records which are still in the threat of getting revealed anytime by anyone.The paper contributes in a way that the record of a singleperson is maintained and stored at a single block then the nextblock will contain the record of the other person and thus forming a chain via implementation of the linked list approach. This may lead to non-redundancy of data that is the availability of duplicate data will also be reduced to a great extent as every block has its hash value which is unique for every block and even if the slightest change would be made to any data the hash will automatically get altered. The objective of the paper can be clearly and precisely highlightedin session III

IV. Results Analysis

As a result of the study, two ways are considered for a blockchain system for any business- one is byuing the cloud application known as G.U Blockchain Cloudand the other by implementing code using any of the programming language such as C, C++, Java, Python. A comparative study is made between a system implementation using blockchain technology and without blockchain technology

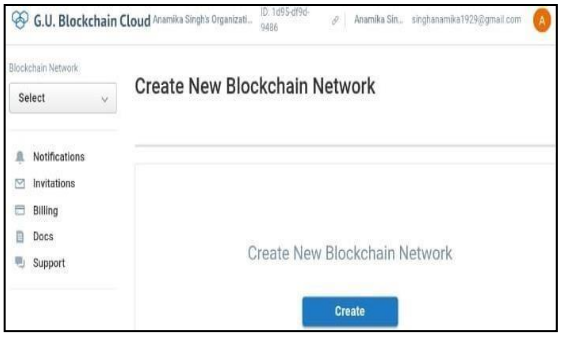
TABLE IV. COMPARATIVE STUDY OF SYSTEMS WITH AND WITHOUT BLOCKCHAIN [27]

Comparison Parameters	Blockchain based system	Systems without blockchain
Confidentiality	This blocks the access of data from unauthorized user owing to public key encryption.	No such enhanced cryptographic technique is used in this approach.
Integrity	By this attribute, blockchain ensures complete access to authorized holder to all the information.	In this approach, still a terror of gaining access of confidential data by an unauthorized user.
Availability	Using blockchain scheme guarantees easy accessing of data to the only those who are allowed.	The confidential data also to be accessed.
Non-Repudiation	It ensures that the results from Consensus Mechanism will remain unmodified.	Due to weak security protocols, this scheme fails to offer unarguable potency of authorship.
Accountability	In these systems full transparency is achieved by moralityof the technology being adopted for use.	Usually don't verify or confirm the strength of procedures and algorithms.

A. G.U Blockchain Cloud

The private and consortium blockchain infrastructure can easily be created with the help of one of the applications for business and to keep data records and can customized the one as per the needs. The application empowering such feature is G.U. Blockchain Cloud. It works in the way that:

- One has to Create an account in G.U Blockchain Cloud

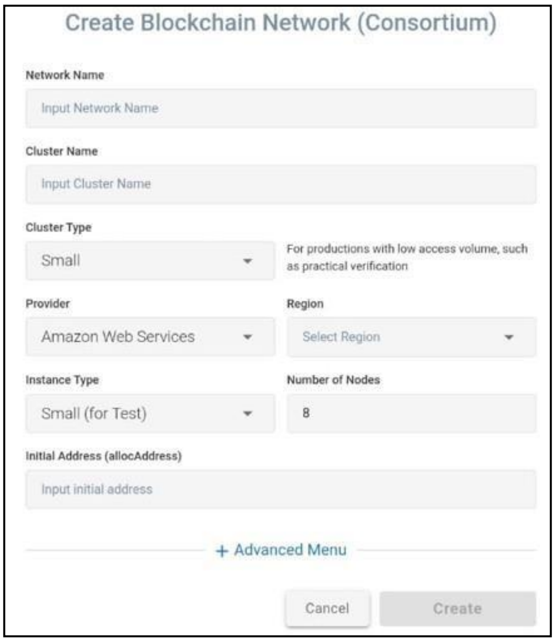


Create New Blockchain Network

Create New Blockchain Network

Fig. 10. Creating new Blockchain Network

- Next, click in create button to create blocks.



Create Blockchain Network (Consortium)

Network Name: Input Network Name

Cluster Name: Input Cluster Name

Cluster Type: Small — For productions with low access volume, such as practical verification

Provider: Amazon Web Services

Region: Select Region

Instance Type: Small (for Test)

Number of Nodes: 8

Initial Address (allocAddress): Input initial address

Fig. 11. Creating new Block for Blockchain Network

V. Conclusion

Traditionally, the records of an individual are maintained on the registers and further the identification was approved by manual signature. With the shifting of traditional paradigm of individual recognition and record keeping from pen and paper to digitalization, the upsurge in the scope and future use is hence witnessed. Biometric ensures security at the ground level but when it comes to storing the data logically, advancements for creating a dataset are needed for that the blockchain technology could be of great use and leads the biometric systems to be more secure and safe for one's identity. The researches in the biometric systems are not new. Past researches were conducted focusing on the physical implementation of the biometric system; how do the functioning and working of a biometrics system occur? What are the issues related to practical implementation? How safe these systems are when comes to identify the individual based on its implementation? But when the backend safety and privacy of the biometric systems is considered, modifications are the prior need for the systems to be more secure ad private. The past researchers and their works recorded and reported that the major issues for not accepting the system is the authorization falsification, and as far as the biometric systems are concerned with the secure and authentic individual identification, the security, integrity and the privacyof the database of biometric system's should be adopted, thus contributing the society with more efficient and trustworthy system

References

[1] https://www.javatpoint.com/biometrics-introduction
[2] Yang, Wencheng, et al. "Securing mobile healthcare data: a smart

cardbased cancelable finger-vein bio-cryptosystem." IEEE Access 6, 36939-36947, (2018).

[3] Zhao, Yikun, et al. "A High-Performance Database Management System for Managing and Analyzing Large-Scale SNP Data in Plant Genotyping and Breeding Applications." Agriculture 11.11, 1027, (2021).

[4] Kok, S. H., et al. "Prevention of crypto-ransomware using a pre-encryption detection algorithm." Computers 8.4, 79, (2019).

[5] Shin-Yan Chiou, "Secure Method for Biometric-Based Recognition with Integrated Cryptographic Functions", BioMed Research International, vol. 2013, Article ID 623815, 12 pages, (2013).

[6] Habibu, Taban, Edith T. Luhanga, and Anael E. Sam. "Developing an algorithm for securing the biometric data template in the database." (2019).

[7] Corso, A. "Performance Analysis of Proof-of-Elapsed-Time (PoET) Consensus in the Sawtooth Blockchain Framework." (2019).

[8] Jiang, Bin, et al. "PIDS: A user-friendly plant DNA fingerprint Database management system." Genes 11.4, 373, (2020).

[9] Naim, Nani Fadzlina, et al. "Mysql Database for storage of fingerprint data." 2011 UkSim 13th International Conference on Computer Modelling and Simulation. IEEE, 2011.

[10] Singh, Yogesh Pal, Santosh Kumar, and Madhulika Singh. "Analysis and Designing A DNA Fingerprinting Based Identifications (DNAFIDs) Model and Database Management System." Reliability: Theory & Applications 16.1 (61) (2021).

[11] Hariharan, R. S., et al. "Face Recognition and Database Management System for Event Participant Authentication." Journal of Physics: Conference Series. Vol. 1916. No. 1. IOP Publishing, 2021.

[12] Kabir, Md Humaun, et al. "Smart Attendance and Leave ManagementSystem Using Fingerprint Recognition for Students and Employees inAcademic Institute."(2021).

[13] Tian, Hongli, et al. "Screening of 200 Core SNPs and the Construction of a Systematic SNP-DNA Standard Fingerprint Database with More Than 20,000 Maize Varieties." Agriculture 11.7, 597, (2021).

[14] Li S, Kot AC. Privacy protection of fingerprint database. IEEE SignalProcess Lett. 18(2):115–8, (2011).

[15] Yang W, Wang S, Hu J, Zheng G. SS symmetry Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry (Basel). (2019).

[16] Elkamchouchi HM. A New Image Encryption Algorithm Combining the Meaning of Location with Output Feedback Mode. In (2018).

[17] Jain AK, Ross A, Uludag U. Biometric template security: Challenges and solutions. In: Signal Processing Conference, 2005 13th European.Citeseer; p. 1–4, (2005).

[18] Emmanuel E, Edebatu D, Catherine N, Ngozi A. Vulnerability of Biometric Authentication System. Int J Innov Res Sci Eng Technol. 2742–9, (2016).

[19] Anitha P, Rao KN, Rajasekhar V, Krishna CH. Security for Biometrics Protection between Watermarking and Visual Cryptography. SSRG IntJ Electron Commun Eng. 64–71, March (2017).

[20] Ashish MM, Sinha GR. Biometric Template Protection. J Biostat Biometric App. 1(2):202, (2016).

[21] Dwivedi R, Dey S, Singh R, Prasad A. A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping. Comput Secur [Internet]. 65:373–86, (2017).

[22] Keerthi, Y., et al. "Enhanced Biometric Attendance Management System using IoT & Cloud." 2022 International Conference on Electronics and Renewable Systems (ICEARS). IEEE, (2022).

[23] M. Faundez-Zanuy, "Biometric security technology," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, no. 6, pp. 15-26,June, (2006).

[24] Habibu, Taban, Edith T. Luhanga, and Anael E. Sam. "Developing an algorithm for securing the biometric data template in the database." (2019).

[25] Shaykh Siddique., Monica Yasmin., Tasnova Bintee Taher., & Mushfiqul Alams, The Reliability and Acceptance of Biometric System in Bangladesh: Users Perspective. International Journal of Computer Trends and Technology, 69(6), 15-21, (2021).

[26] Pujari, Mr Vinayak, Rajendra Patil, and Mr Shailesh Sutar. "Research paper on biometrics security." *Contemporary Research in India* (2021).

[27] Suman Mann, Tanya Jain and Aakash Vyas. The Blockchain Revolution: Paradigm Shifts in Traditional Voting Practices. *International Journal of Computer Applications* 176(37):36-42, July, (2020).