Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 2, August 2023
Paper : 16

Securing Biometric Information Using Block Chain

1. Chandiraprakash.N ,Assistant Professor, Department of CSE(AIML),
2. Malla Reddy Institute of Engineering and Technology (Autonomous), Telangana, India. chandrunit26@gmail.com 0000-0003-4276-0289 - ORCID NO
3. Dr.Vijayakumar.K, Assistant Professor(Sr.G), Department of Computational Intelligence, School of Computing, SRM Institute of Science and Technology, SRM nagar, Kattankulathur,Tmilnadu, india. vijayakk1@srmist.edu.in 0000-0002-1473-385x - ORCID NO
4. Dr.Manikavelan.D , Professor in the Department of CSE, Saveetha School of engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
5. Dr.S.ManthandiPeriannasamy, Professor, Electronics and Communication Engineering, Mallareddy Engineering College For Women, Maisammaguda,Hyderabad.
6. R.Geetha, Assistant professor, Department of IT,Malla Reddy Institute of engineering and technology, Telangana,India.
7. Dr JayaprakashC, Professor of CSE,Malla Reddy College Of Engineering For Women Maisammaguda, Medchal - 500100, Telangana, INDIA
8. A.Kavya, 2ND year Of CSD, Malla Reddy Institute Of Engineering and Technology, Telangana, India.

ABSTRACT

Biometrics, with its distinctiveness to each independent, has been modified as a security attestation function via way of means of number of institutions. This kind of biometric statistics are processed into templates which might be stored on the databases, and a government concentrates and manages those databases. This method of preserving biometric statistics, or in our case of fingerprint template, is uneven and has three types of main security protection attacks, together with faux template input, template change or removal, and route of the interception via way of means of a malicious attacker. In this paper, we stable an encrypted fingerprint template via way of means of a symmetric peer-to-peer community and symmetric encryption. The fingerprint is encrypted via way of means of the symmetric key set of rules: Advanced Encryption Standard (AES) set of rules after which is uploaded to a symmetrically allotted to distributed storage device, The hash of the template is stored in a decentralized block chain. By acquiring the proposed device which supports template hashing which leads to cost- powerful and coherent. The experimental results illustrate that the proposed tool secures the fingerprint template via means of encryption, hashing, and decentralization.

INTRODUCTION

Biometrics are a way to measure a person's physical characteristics to verify their identity. These can

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 2, August 2023
Paper : 16

include physiological traits, such as fingerprints and eyes, or behavioural characteristics, such as the unique way you would complete a security-authentication puzzle. Biometrics has the potential to make authentication dramatically faster, easier and more secure than traditional passwords. Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Typically, biometric authentication is used to manage access to physical and digital resources such as buildings, rooms and computing devices. The security of the biometric authentication data is vitally important, even more than the security of passwords, since passwords can be easily changed if they are exposed. A fingerprint or retinal scan, however, is immutable. The release of this or other biometric information could put users at permanent risk and create significant legal exposure for the company that loses data. Blockchain is a specific type of database. It differs from a typical database in the way it stores information; blockchains store data in blocks that are then chained together. As new data comes in it is entered into a fresh block.

Once the block is filled with data it is chained onto the previous block, which makes the data chained together in chronological order. By design, a blockchain is resistant to modification of its data. This is because once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks. The resulting hybrid biometric system would be more secure. However, this is not an easy goal to achieve. all the computation performed in a public blockchain is accessible to every participant. This makes necessary to use non-standard encryption or other protection techniques to manage the biometric data in the blockchain. This is specifically relevant when incorporating biometrics to blockchain, as biometrics are private data in many cases sensitive. With blockchain-infused biometrics identity systems, the authorized individual has complete control of the decentralized, distributed ledger and can also actively view who accesses and shares the data within the ledger. The integration of biometrics and blockchain technologies (public and private) has multiple complex elements and implications in security, storage, and beyond.

Problem Statement

The aim of the project is to secure the individuals information or any private data by securing it along with the fingerprint using block chain. As we all know in this growing technological world there will be always advantages as well as disadvantages. Usually, people wanted to protect their personal information or data in a secure manner but in most of the case they chose centralized database to store their information for ex even our government keeps all the data of each and every individual like Aadhar card number in centralized data base system which can be easily go through the security attacks, as malicious attackers can easily decode and can get the information from the centralized database system. In most of the organization they use traditional method to store information including fingerprint and retinal scan data in it as it is meant to be the most important and personal data of every individual as the fingerprint, that's a shape of biometrics which is used for safety authentication in maximum high-level safety establishments or any other organizations. The

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 2, August 2023
Paper : 16

traditional tactics of shielding one's privacy, including Passwords, tokens, and key code, had been slowly removed with the creation of fingerprint, as it's unique for each and every individual and secure the data very productively. The fingerprint template is generally saved in a centralized database, which increases the hazard of spoofing, facts tampering, identification theft, and channel interception. As this is very important and necessary that it should be secured and protected so that it cannot be retrieved by the hackers

Existing System

The existing method which includes several techniques for securing personal data or information by using the decentralized storage system that is nothing but the block chain. As Block chain is a kind of shared database that differs from an ordinary database in the way that it stores information; block chains save data in blocks which are then connected to cryptography.

Block chain is among the rising technology which have a relatively robust cryptographic basis that allows packages to leverage its capabilities to obtain resilient safety solutions as we use data hashing technique which is cost-effective and efficient. Using Block chain method, we are trying to secure the finger print template along with the personal information of that particular person with the help of hashing techniques. The integration of biometrics and block chain technologies (public and private) has multiple complex elements and implications in security, storage, and beyond.

Proposed System

Proposed system is by using the biometric to secure the data of each and every individual in the block chain system. Here hashing techniques are used to keep the data in the encrypted format by which nobody will be able to decode the data and each encrypted data will be stored in the block connected in the chain by which it will become more difficult to change the content present in that as each block in the chain accommodates a number of transactions, and every time a new transaction takes place on the block chain, a record of that transactions is appended to every participant's ledger. The decentralized database managed with the useful resource of the usage of numerous contributors and is called as Distributed Ledger Technology (DLT). The transactions are recorded in the form of DLT in a Block chain that may be recorded with having some cryptographic Signature. Block chain transactions takes place within peer-to-peer network of globally distributed computers (nodes). Each node maintains a copy of the block chain and contributes to the functioning and security of the network.

Objective

The main objective of the project is to develop a model where one can easily secure their personal information or data in the decentralized database rather than the traditional database system which is not meant to be safe. Here anyone can secure their data just by using their fingerprint, then uploading the personal data or information in the block chain where the data will be converted into encrypted form by using the hashing technique which can then be retrieved by using the same finger print of that particular person who wanted to see his stored information in the block chain. Here along with the

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 2, August 2023
Paper : 16

data, fingerprint templates are also secured by using the encryption method.

LITERATURE SURVEY

1. Block chain in Biometrics

In 2018, the authors in [14] proposed a system to secure fingernail data where the management center is simulated while using node.js. This system comprises a data management system that acts as nodes responsible for storing fingernail data sent by device nodes, which is responsible for pre-processing the captured fingernail from the user. The idea of off-chain (i.e., processing data off the block chain) is adapted into this paper because of the workload that is incurred by nodes if they were storing and processing the fingernail template. Shih et al. proposed system use the "full chain" technique (i.e., pre-processed data is stored in all the data centers) of storing the fingernail template

2. The concept of using the "side chain" of processing data

It is discussed in [13], which combines the users' fingerprint template and other user data and saves it on the side chain, which is then compared to the "Aadhar card number" on the "main chain." This method is effective in eliminating congestion. The authentication of a user is done by comparing the details on the Ethereum network.

3. Patients are authenticated by using the block chain network to store encrypted hybrid patterns of the patient.

This hybrid pattern consists of the RFID and the finger-vein feature of the patient processed and hashed while using the MD5 and AES algorithm. This makes attacks, such as brute force attack and spoofing, near to impossible. The processed data are sent from the access node to the block chain to be stored and later authenticated if a patient enrolls.

4. The use of a biometric e-ID in a system to validate users during voting using the block chain technology

It was proposed in [15] to solve the malicious attack on the previous system. This system is secure, because citizen information is combined with fingerprint data and later uploaded onto the block chain network, in order to authenticate registered citizens.

5. Patients are authenticated by using the blockchain network to store encrypted hybrid patterns of the patient. This hybrid pattern consists of the RFID and the finger-vein feature of the patient processed and hashed while using the MD5 and AES algorithm. This makes attacks, such as brute force attack and spoofing, near to impossible. The processed data are sent from the access node to the blockchain to be stored and later authenticated if a patient enrolls.

6. The use of a biometric e-ID in a system to validate users during voting

Using the blockchain technology was proposed in [5] to solve the malicious attack on the previous system. This system is secure, because citizen information is combined with fingerprint data and later uploaded

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 2, August 2023
Paper : 16

onto the blockchain network, in order to authenticate registered citizens

SCREENSHOTS

8.1 Home Page

Figure 8.1: Home Page

The Figure 8.1 shows the homepage of the application.

8.2 Login Page

Figure 8.2: login page

Figure 8.2 shows the login page of the application

8.3 Student details page

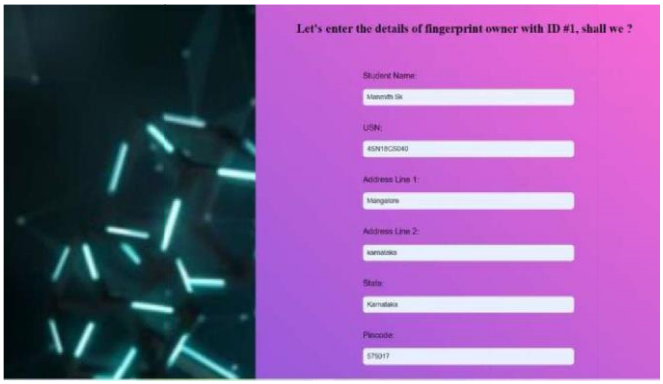

Figure 8.3: student details page

Figure 8.3 shows the form for filling the details

8.4 Result Page

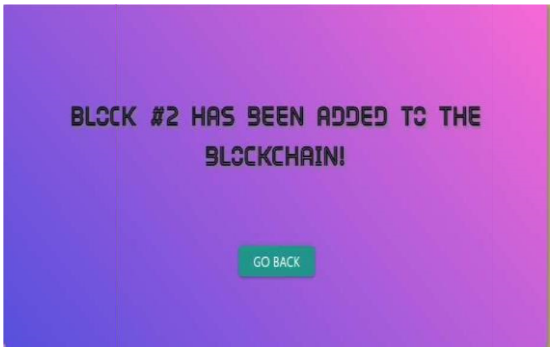

Figure 8.4: Result page

Figure 8.4 shows the successful addition of block where the information of particular student is stored.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6- Issue 2, August 2023
Paper : 16

8.5 Retrieved Page

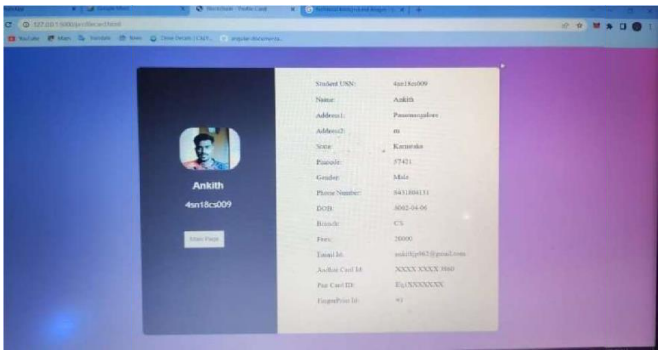

Figure 8.5: retrieved page

Figure 8.5 here stored information will be retrieved from the block chain

8.6 Integrity check page

Figure 8.6: Integrity page

Figure 8.6 here check the integrity of the block chain as whether it is modified or not.

8.7 Arduino kit

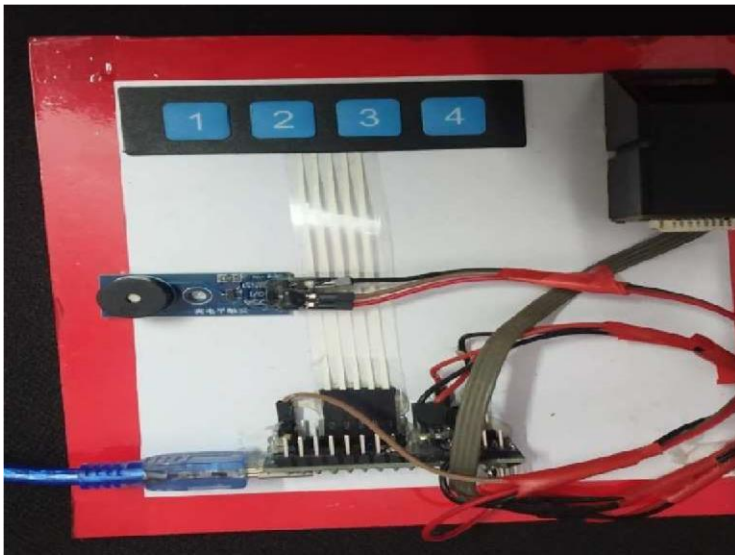

Figure 8.7: Arduino kit

Figure 8.7 shows the arduino kit along with the buzzer, some useful buttons and fingerprint scanner

8.8 Teraterm Software

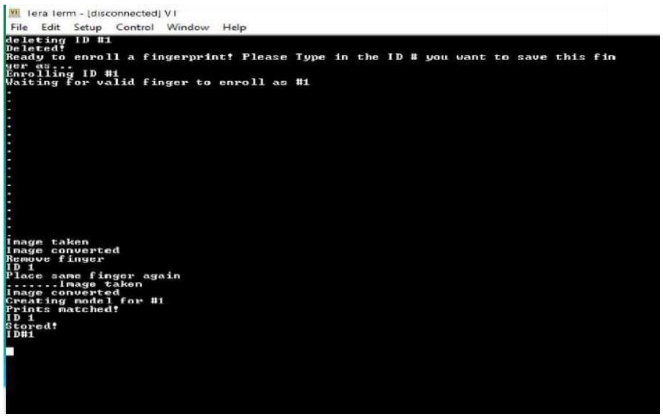

Figure 8.8: Teraterm software

Figure 8.8 here we can store the fingerprint id, match the fingerprint id and delete fingerprint ID.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 2, August 2023
Paper : 16

SECURITY ANALYSIS OF THE IMPROVED SYSTEM

The merits of our proposed system are laid out in this section. The traditional fingerprint data storage system is vulnerable to various attacks, and we analyze such attacks and how our proposed system solves them.

Template database attack

The fingerprint database has a centralized data storage system, which results in the loss of data or user information theft. Our system proposes the use of Blockchain technology which stores the data by splitting it onto different nodes. The difficulty of attacking every node on the system is tremendous and encrypting
the template makes it more difficult.

Upload of fake template

Spoofing of a fingerprint system has long been an issue, and malicious attackers have resulted in this method to bypass the most secured systems. Therefore, we upgraded the system in order to eliminate this problem by utilizing the Blockchain network. The immutable feature of the Blockchain network which ensures that
all transactions cannot be changed

Channel interception

Middlemen or DBA turn to handle database or cloud storage for the traditional fingerprint system and, thus, given the authority to manipulate data or even sell user information. The Facebook-Cambridge analytica scandal proves the disadvantage of centralized data storage or including middlemen. If a malicious node on the proposed system tries to alter the block chain for benefits, it will result
in being unsuccessful, because block chain are tamperproof once deployed.

CONCLUSION AND FUTURE SCOPE

In our project we have implemented a fingerprint template to store the personal information and use the same fingerprint template to retrieve back the data from the block chain. We implemented a python application in the platform VS code. Live dataset is used in the project.
Here block chain technology is used to store the personal data or information using the fingerprint template. Our main motto is to secure the data in the decentralized database rather than centralized database as it is more secure as compared to it. Here with the help of fingerprint template we are trying to store the data in the block chain. Future work may include advanced integrity check where one can able to know the integrity of the chain as whenever any attacker try to hack the block in future then it should give an alert message telling that someone is trying to modify the block. Also one can use as the mobile application to store the personal data or information using the fingerprint scanner in it.

REFERENCES

[1] A.H, Rubab, S and Jhat, Z.A. Journal of Computing and ICT Research, Vol.5, Issue 2, pp 6780.

[2] Ravi Subban and Dattatreya P. Mankame, Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013.

[3] D.Vinitha, P.V Ramesh, International Journal of Computer Science and Engineering, Vol 7,Special Issue, 6, March 2019

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 2, August 2023
Paper : 16

[4] Elena Pagnin and AikateriniMitrokotsa, Hindawi Security and Communication Networks, Volume 2017, Article ID 7129505.

[5] Páez, R.; Pérez, M.; Ramírez, G.; Montes, J.; Bouvarel, L. An Architecture for Biometric Electronic Identification Document System Based on Blockchain. Future Internet 2020, 12, 10. [Google Scholar] [CrossRef].

[6] Anil K. Jain, KarthikNandakumar and Abhishek Nagar," Biometric Template Security", Schlossdagstuhl Leibniz centre for informatics.

[7] V. Evelyn Brindha , "Biometric security using fuzzy vault " IEEE 15th International Symposium on Consumer Electronics (ISCE).

[8] Oday A. Hassen, Ansam A. Abdulhussein, SaadM. Darwish, Zulaiha Ali Othman, Sabrina Tiun and Yasmin A. Lotfy," Secure Signature Scheme Based on Multimodal Biometric Technology", MDPI Journals.

[9] Geeiharamani R, 8alanibiamanian U. Automatic segmentation of blood vessels from retinal fiindusimages through image process ingand data mining techniques. Sadhana. 2015 Sep

[10] Oday A. Hassen, Ansam A. Abdulhussein, Saad M. Darwish, Zulaiha Ali Othman, Sabrina Tiun and Yasmin A. Lotfy," Secure Signature Scheme Based on Multimodal Biometric Technology", MDPI Journals.

[11] Zibin Zheng, ShaoanXie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang International Journal of Web and Grid Services, Volume 14, No. 4, 2018.

[12] Hye-Young Paik 1,2, XIWEI XU 1,2, H. M. N. DilumBandara 1, Sung Une Lee 3, and Sin Kuang Lo 1,2 December 2019 IEEE Access PP (99):1-1, Volume 7, 2019.

[13] Lee, S.H.; Yang, C.S. Fingernail analysis management system using microscopy sensor and blockchain technology. Int. J. Distrib. Sens. Netw. 2018, 14, 1550147718767044. [Google Scholar] [CrossRef].

[14] Pawade, D.; Sakhapara, A.; Andrade, M.; Badgujar, A.; Adepu, D. Implementation of FingerprintBased Authentication System Using Blockchain. In Soft Computing and Signal Processing; Springer: Berlin/Heidelberg, Germany, 2019; pp. 233–242. [Google Scholar].