Grenze International Journal of Engineering and Technology, Jan Issue

Blockchain Encryption using Biometric Authentication

Anjani Nandan[1], Abhishek kumar[2], Parth srivastava[3], Shivateja Chalvadhi[4] and Neha Hajare[5]
[1-5]School of Computer Engineering and technology, MIT Academy of Engineering, Pune412105, India
Email: anjaninandan1234@gmail.com, abhishekkumarraj838@gmail.com, davparth@gmail.com, shivatejachalvadhi@gmail.com, nphajare@comp.maepune.ac.in

***Abstract*—Due to increase in the data breaches over the last few years and even the initial layers of authentication failed to stop the data breaches its been crucial to take a step forward and bust the cyber frauds and maintain the confidentiality and integrity of the user.To Achieve the cyber goals in this paper we presented an idea of eliminating a central authority by keeping a decentralized system so that the attacks on server can be totally eliminated and therefore To tackle the data breaches by implementing the blockchain architecture ,each node will be user and will be storing the information of the previous node in the network.to add one more layer of authentication that is Biometric .Data of the user will remain secured and if the biometric identity is compromised losses will be very less compared to centralized system also the information of biometric data is way more secured.**

***Index Terms*— Blockchain,BiometricAuthentication,Minutiae Algorithm,DES.**

I. Introduction

Information is present in all areas of life .The models used in the past years are most of the things remote. the main building block has been authentication in the system .Nowadays we are seeing in making transaction apps like phonepe and paytm are using technology like Biometric authentication but still the cyber criminals are able to make breaches so to make the system more secure we have proposed a new system of authentication adding one more layer of security that is blockchain.The basic aim of this project is to develop a multilayer authentication system which can minimize the threats or data breach or cyber attacks while doing any transaction ,sending mails etc. and If you ask Why did we select biometrics?Because OTP can be easily attack by the third person and also the OTP is accessible to the service providers so they can violate the goals of authenticity whereas the data stored in blockchain cannot be easily tampered and hence acts as a secure storage when compared to other available options.Data of the user will remain secured and if the biometric identity is compromised losses will be very less compared to centralized system also the information of biometric data is way more secured.Looking all the layers it won't be wrong to say that we are adding there will be authenticity and the user has to pass through different players to get the accessibility .

II. Related Work

FA works by adding an extra layer of security i.e a passcode or password to the pin so that it becomes hard for the hacker to

The survey found many attacks which have become popular in the past years MITM: The attacker interrupts messages in the middle of its transmission and tries to cheat the communicating parties by posing as a third

Grenze ID: 01.GIJET.9.1.530

party.[1]SIM swapping and hacking: Threat actor convinces your carrier to switch your number to a SIM that the attacker own.Lost and synced devices: possibility to sync SMS messages with other devices.Phishing: Social engineering and impersonation.Account takeover: Access to SMS through service provider portal. Reliability:SMS Delay and Loss: According to a study by keynote systems(94.7% of the SMS messages arrive at their destination in an average of 11.8 seconds. This means 5.3% arrives late or do not arrives at all !)
Coverage : In order to receive the SMS OTP, you have to be in area with cellular coverage with carrier acceptance
Dependency: High dependency on multiple parties starting from the SMS gateway reseller, SMS aggregator, Telecom provider, Client phone.So, that we conclude that SMS OTP vulnerable to several types of attacks.SMS OTP is costly and not reliable.Sandeep Shiravale [14] Blockchain technology will help make data more reliable and secure, preventing the loss of data and unauthorized access. Consensus algorithm along with the hash algorithms maintains the integrity of data while providing authentication and authorization. The Identity Based Encryption management concept allows the encryption of the user's data as well as their identity..Shrikant Salve[13] Many government websites and systems were hacked in the past few years.go to analyze study on various cyber-attacks that were triggered in India and other countries. Also, in this paper, we have reported a proposed intelligent system which is based on supervised and unsupervised learning techniques.

III. METHODOLOGY

Authentication technique	Input	process	Output
password and username verification	user fill the form by giving information of username and password	the entered form details matched with the server database and replies yes or no	user will be redirected to another page for OTP verification
Biometric Identification and verification (2nd layer)	user need to save his finger print in biometric to access this application	finger prints would then be matched with the stored ones through database and the result being yes or no would be reflected on the screen	user will be redirected to the main page after successful verification
4t 2nd layer (Blockchain Messaging)	user will enter message	DES encryption and SHA will encrypt and create hash	message hash value will get generated and user can continue doing messaging blocks will be keep on generating

A. Algorithms

1.For BIometric Encryption refer figure 1 - minutiae Algorithm used , Compared to previous fingerprint representations, the minutiae are more stable and resistant to contrast, image resolutions, and global distortion. Even though the majority of automatic fingerprint identification systems are built to employ minutiae as the primary fingerprint feature for detection, extracting the minutiae from a low quality image is a difficult operation.

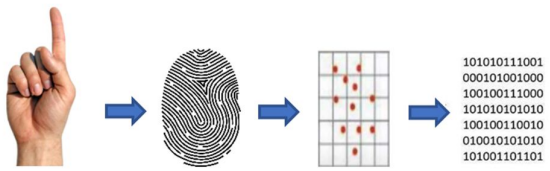

Fig. 1 Fingerprint working architecture

For message encryption - DES ALgorithm

Refer fig 2 A team from IBM developed the DES (Data Encryption Standard) algorithm, a symmetric-key block cypher that was later accepted by the National Institute of Standards and Technology (NIST). The algorithm creates ciphertext from the plain text in 64-bit blocks.using 48-bit keys then it it further permuted goes and then

for decryption same key is used.

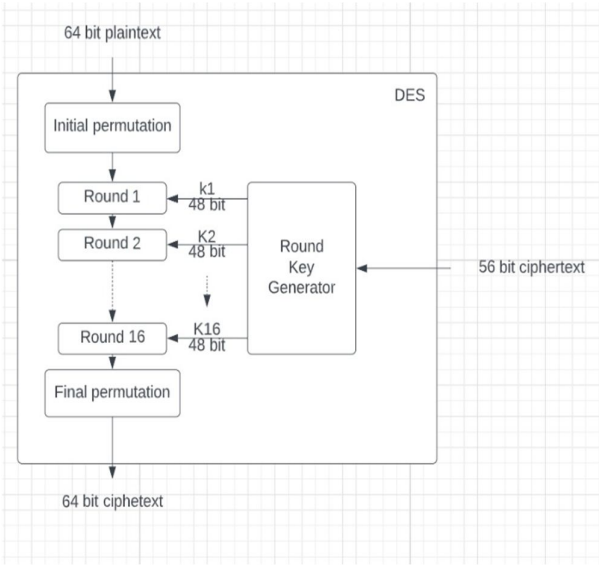

Fig.2 - DES working architecture

ref fig 3 For message hashing we have used - SHA, or secure hashing algorithm, stands for. Data and certificates are hashed with SHA, a modified version of MD5. By utilising bitwise operations, modular additions, and compression functions, a hashing algorithm reduces the input data into a smaller form that is impossible to comprehend.

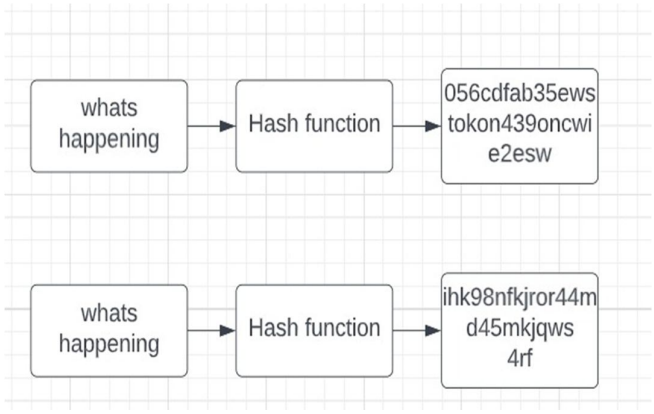

Fig-3 generation of hash value indicating how different hash values are getting generated

IV. Results and Discussion

Refer figure 4 and 5 First we need to enter data and it will shows you the hash value. if you want data also in encrypted format then you need to select the encrypt symbol then you need to enter the data then it will also encrypt the data also and it will generate hash value with data encryption value.

V. Conclusion

As we mention that you project is keep data confidential so using our app we can keep the data safe as our project is to build a blockchain encryption with biometric authentication with the help of this if want to send any data to another person you just need to enter your data in this app and it will generate hash value if you think hash value can also generated by online tools and also can be crack by online tools yes it can be crack or can be created by online tools but we are generating hash value through blockchain so it will impossible for any online

tools to generate this with blockchain and they also cannot able to crack this . so using this app we can provide confidentiality and integrity to you .

Fig. 4 BlockChain Application

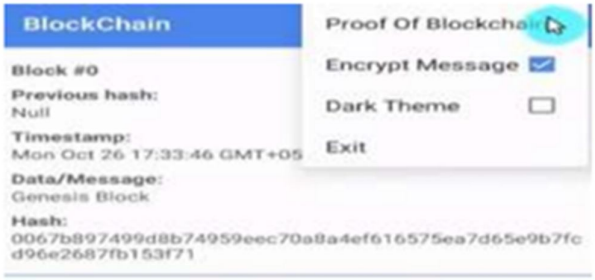

Fig. 5 Blockchain Encrypt Message

ACKNOWLEDGMENT

Thank you to everyone who contributed to your project.
We would like to convey our gratitude to Mrs. Neha Hajare, our recognised project advisor and guide, for her unwavering support and invaluable advice throughout the execution of this project work. Additionally, we would like to thank esteemed School Dean Mrs. Ranjana Badre for her unceasing support. If we didn't express our gratitude to the rest of the professors and staff for their wise counsel and steadfast cooperation, we would be failing in our responsibility.

REFERENCES

[1] Tyagi, P. B. Singh, V. S. Yadav, S. K. Singh and A. Tiwari, "Security role of biometrics in electronic transactions," 2012 IEEE International Conference on Computational Intelligence and Computing
[2] Hassan, A. George, L. Varghese, M. Antony and K. K. Sherly, "The Biometric Cardless Transaction with Shuffling Keypad Using Proximity Sensor," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020

[3] Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. -K. R. Choo and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2146-2156, Aug. 2020, doi: 10.1109/JBHI.2020.2969648.7
[4] Thuraisingham, "Blockchain Technologies and Their Applications in Data Science and Cyber Security," 2020 3rd International Conference on Smart BlockChain (SmartBlock), 2020, pp. 1-4, doi: 10.1109/SmartBlock52591.2020.00008.3
[5] Q. N. Tran, B. P. Turnbull and J. Hu, "Biometrics and Privacy-Preservation: How Do They Evolve?," in IEEE Open Journal of the Computer Society, vol. 2, pp. 179-191, 2021, doi: 10.1109/OJCS.2021.3068385.
[6] R. Youmaran and A. Adler, "Measuring Biometric Sample Quality in Terms of Biometric Information," 2006 Biometrics Symposium: Special Session on Research at the BiometricConsortium Conference, 2006, pp. 1-6, doi: 10.1109/BCC.2006.4341618
[7] A. Thawre, A. Hariyale and B. R. Chandavarkar, "Survey on security of biometric data using cryptography," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 2021, pp. 90-95, doi: 10.1109/ICSCCC51823.2021.947812
[8] V. Naidu, K. Mudliar, A. Naik and P. Bhavathankar, "A Fully Observable Supply Chain Management System Using Block Chain and IOT," 2018 3rd International Conference for Convergence in Technology (I2CT), 2018, pp. 1-4, doi: 10.1109/I2CT.2018.8529725.
[9] L. Xiaoling and L. Zhaoyang, "Research on agricultural product traceability system based on block chain technology," 2020 International Conference on Computer Science and Management Technology (ICCSMT), 2020, pp. 318-322, doi: 10.1109/ICCSMT51754.2020.00072.
[10] T. Salman, R. Jain and L. Gupta, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 520-527, doi: 10.1109/Blockchain.2019.00078.
[11] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 184-193, doi: 10.1109/Blockchain.2019.00032.
[12] H. Desai, M. Kantarcioglu and L. Kagal, "A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 34-43, doi: 10.1109/Blockchain.2019.00014.
[13] A. S. Choudhary, P. P. Choudhary and S. Salve, "A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 612-617, doi: 10.1109/ICICT43934.2018.9034445.
[14] S. Khan, A. Jadhav, I. Bharadwaj, M. Rooj and S. Shiravale, "Blockchain and the Identity based Encryption Scheme for High Data Security," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 1005-1008, doi: 10.1109/ICCMC48092.2020.ICCMC-000187.