iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48222

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

Instant and Secure Messaging Platform Based on Blockchain

Ajay Kumbhar[1], Madhav Godale[2], Payal Jagtap[3], Amruta Misal[4], Mr. Abhijeet Cholke[5]
[1, 2, 3, 4]*Computer Department Trinity Academy Of Engineering, Pune, India*
[5]*Asst.Prof. Computer DepartmentTrinity Academy Of Engineering, Pune, India*

Abstract: ***In recent years, texting and messaging have become more prevalent than face-to-face communication, and users are becoming increasingly aware of data privacy issues associated with them. Therefore, a secure and simple way to connect is crucial for individuals and organizations with different identities and goals. The most popular organization messaging applicationsare moving towards end-to-end encryption (E2EE) as a means of ensuring the privacy and security of their users. As a result of theimplementation of the messaging distributed application, several benefits will be brought to society and the way information or different services are handled. The main objective is to develop the chatting platform to increase the privacy of messages. Consequently, both organizations and individuals express deep concern regarding the security of data and privacy when using instant messaging applications. This research seeks to enhance the security channels in chat platforms by using a new technology such as blockchain. Blockchain is a technology that operates on a decentralised basis. By overcoming the disadvantages of traditional messaging applications, we can ensure official data's confidentiality, integrity and availability, as well as advancedauditing capabilities.***

Index Terms: Blockchain, secure messaging, encyption, E2EE,instant messaging

I. INTRODUCTION

Social interaction and leisure time have changed culturally as a result of the development of the Internet and social media. More than 4 billion people use messaging apps every month worldwide. Instant messaging enables real-time com- munication between two or more Internet users. However, the instantaneous and interactive features of mobile applications (apps) made them a desirable option for corporate teams' or organisations' instantaneous communications.

People and companies may now connect with one another us- ing a range of apps like WhatsApp and Viber as well as within organisations using apps like Microsoft Teams and Skype for Business thanks to the high adoption rates of instant messagingservices in many countries etc. Nowadays, most managerial or company choices are made through mobile communications, and these crucial judgments should be precise and traceable. Users of these platforms for instant messaging will be ableto communicate in real time with two or more people.

Be- cause messaging is more handy than other communication channels, even businesses prefer it to emails and business letters. However, the messaging platform must have adequate security to prevent unauthorised users from accessing the commercial chats. There may be severe repercussions for the over 200 million people who use instant messaging while at work. Instant messaging serves as a backdoor for businesses, rendering IT systems useless.

TUsers of these platforms for instant messaging will be able to communicate in real time with two or more people. Because messaging is more handy than other communication channels, even businesses prefer it to emails and businessletters. However, the messaging platform must have adequate security to prevent unauthorised users from accessing the commercial chats. There may be severe repercussions for the over 200 million people who use instant messaging while at work. Instant messaging serves as a backdoor for businesses, rendering IT systems useless.

In addition, there is a speed constraint with ChatApp since each transaction takes about 30 seconds to complete. Overall,a more secure chatting application is introduced that provides its users a higher level of privacy compared to commonly used messaging applications.

This system places a strong emphasis on decentralised methods, which allows users more security and privacy. An automated mechanism known as a smart contract facilitates transactions between two parties without the involvement of a third party. Once the organization's smart contract is implemented on the blockchain network, it becomes independent of its developers and is impervious to outside manipulation. The user feels extremely secure using this method

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

II. RELATED WORK

A number of sectors are looking into blockchain-based technological solutions that can boost efficiency, streamline business operations, and deliver great trust between persons with little to no prior knowledge. On the other hand, a peerto- peer chat system tries to replace the centralized server with decentralized servers located on each user's device. Due to these peer-to-peer decentralized systems' increased scalabilityand security, the demand for privacy and data security has increased significantly.

They present the idea of a decentralized messaging platform using a stream cipher algorithm. And gives the whole overviewof this project and how it works, it has to establish in a proper way which helps us to create a decentralized messagingplatform having more security [1].

They show to present a decentralized messaging system basedon blockchain technology. This system allows their users to securely send and receive digital messages in the network. Since the messages stored in a conventional blockchain could be easily read by everyone in the network, under the pro- posed approach these messages are previously encrypted using public-key cryptography, while the sender and recipient remainanonymous [6].

They present the idea of smart contracts i.e., Communicaion between contracts takes more gas than method calls within a single contract. Also, every separately deployed contract inthe system increases the overall attack surface. And gives details about a Smart contract are simply programs storedon a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss [2].

They have proposed a blockchain-based End-to-End Encryp- tion framework that can mitigate many of the contemporary vulnerabilities. Any user can fetch the certificate for another user from the application server, and communicate securely with them using a ratchet forward encryption mechanism. From this, we get brief details about the encryption processes how to encrypt the message and how to decrypt the message using the key generator algorithms and the help of stream cipher or block cipher [3]

III. METHODOLOGY

As you can see the above figure there are two user one is sender and other is receiver. As the sender send some text or message to the receiver at first we call that as a plain textwere after that we have to encrypt the message or text for that we have to generate the key for the encryption process. To generate the key we have many algorithms such as SHA-256, MD5, ECC etc.

We are using here SHA-265 algorithm for key generation after the key is generated, we add the key to the plain text or message to encrypt, This process is known as Encryption. Theresult of encryption is later known as cipher text as shown is figure above. The cipher text is non readable has it contains of hash value(numeric value). So, if any third party tries to accessthe message or text then they won't be able to see because of encryption the plain text or message is already converted into numeric value that needs the key to decrepit it.

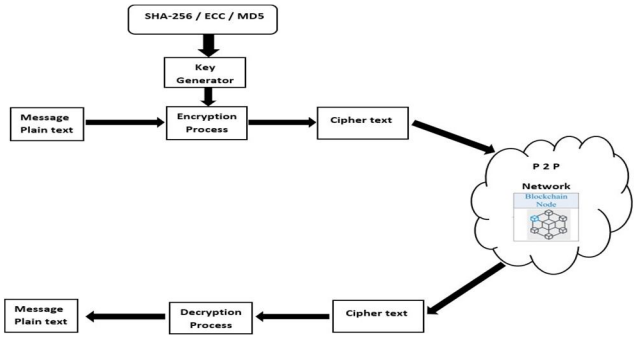


Fig. 1. Block Diagram

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as public distributed ledger. The blockchain is a type of distributed ledger technology (DLT) that consists of growing list of records known as blocks, that are securely linked together using cryptography. each block contains a cryptographic hash of the previous block, they effectively form a chain with each additional block linkingto the ones before it. the data in any block cannot be altered without altering all subsequent blocks.

As receiver gets the cipher text it needs a key that will decrypt the text into a readable format. As in receiver sideit uses private key to decrepit the plain text that is known as decryption. After the decryption process the receiver is ableto see the text or message that is send by the user(sender).

A. System Consists of the Following Modules

1) *Encryption Process:* This is used to encrypt the plain text message. In that process, the plain text message is got and on that plain text message, the key gets applied to that plain text message with the help of stream cipher or block cipher plain text message gets converted into cipher text which can't be readable in that form.

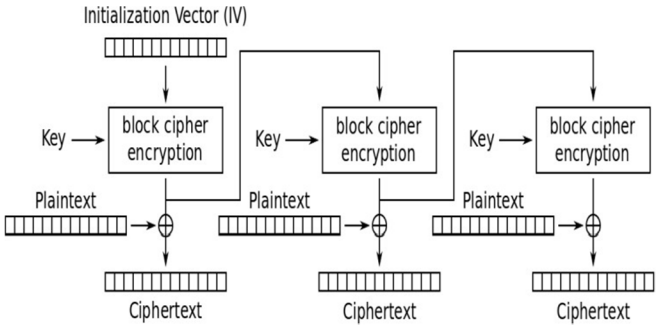


Fig. 2. Encryption process

2) *Key-Generator:* After the plain text message come to the encryption process there will be a key applied to that plaintext message. that key is generated by the cryptographic algorithms. The basic key generator cryptographic algorithms are SHA-256, MD 5, and ECC. The cryptographic algorithms have some specific size, and on basis of that size, the hash value gets generated. Basically, SHA-256 is 256 bits and MD5is 128 bits.

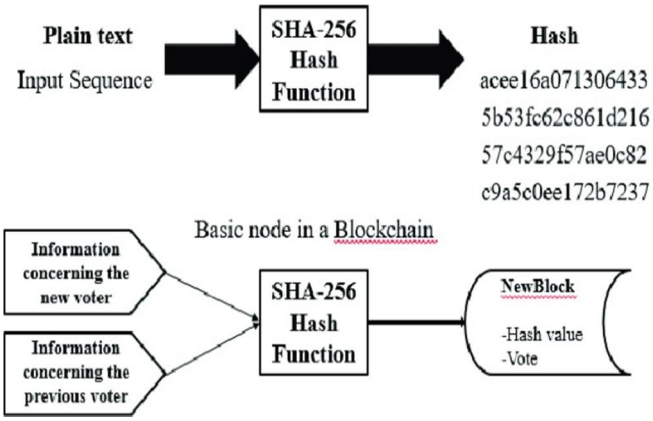


Fig. 3. Decryption process

3) *Blockchain Network:* separate terms, 'block' and 'chain'. A block being referred to a collection of data, alias data records, and a chain being referred to a public database of these blocks,stored as a list. These lists are linked using cryptography,making it the most essential and fundamental requirement for creating a blockchain. Blockchain is a growing list of records, and the blocks get appended to the list with time.

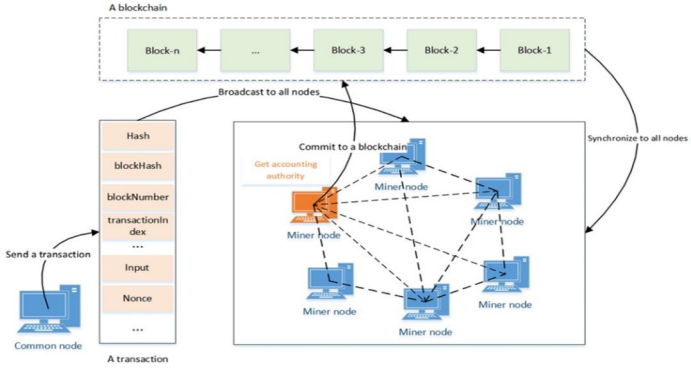


Fig. 4. Decryption process

4) *Decryption Process:* In the deryption process cipher text gets fetched from the blockchain network. this cipher text is in an encrypted form we have to decrypt them for decryption there is one key that is shared by the cryptographic algorithm by applying that key the cipher text gets in the normal form and then it's shown to the user display in a plain text message.

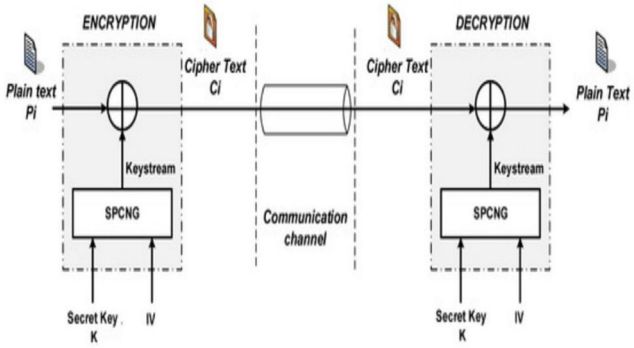


Fig. 5. Decryption process

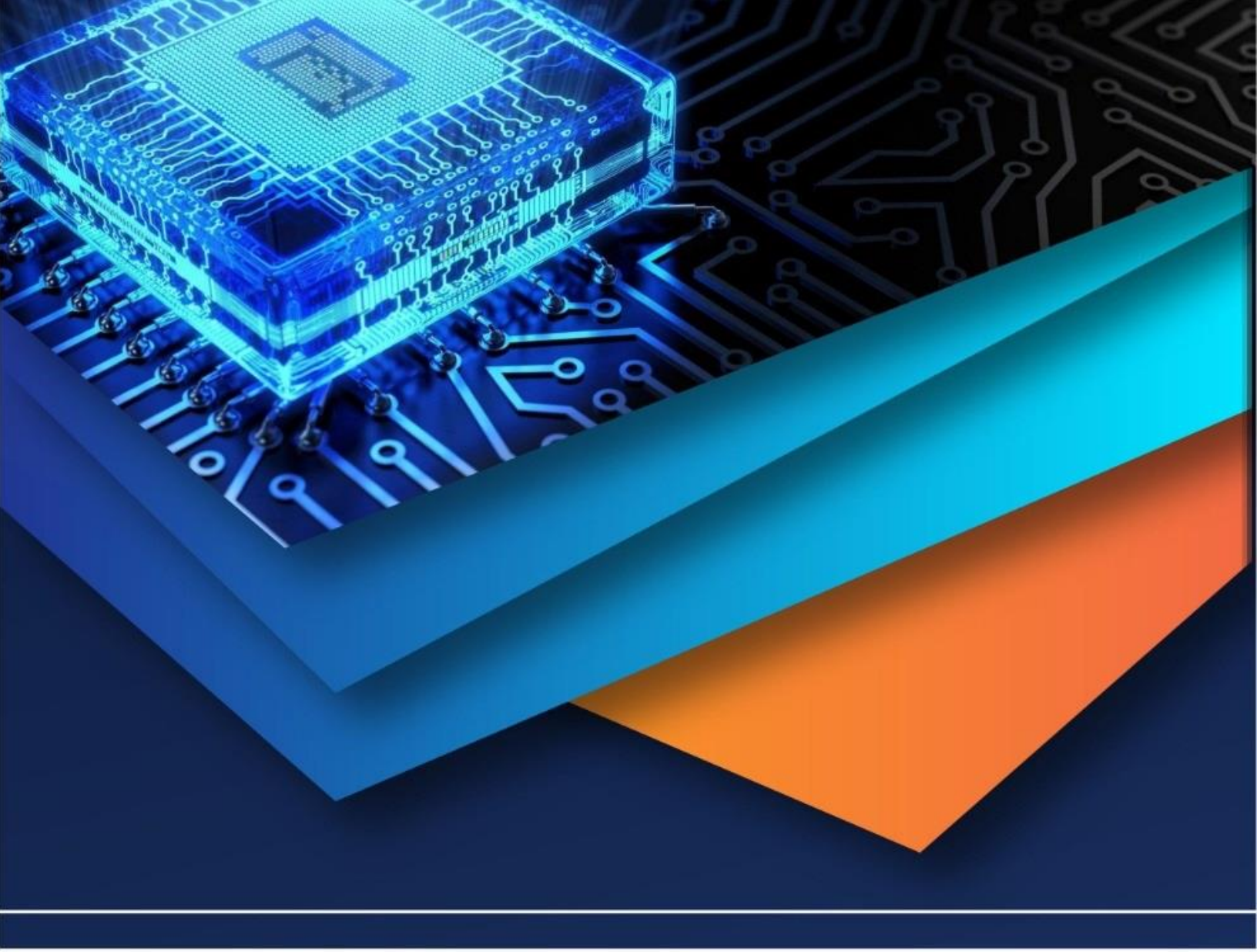
So here below we have given the comparison between the two algorithm and on the basis of this we have decided to choose SHA256 algorithm for our project.

Key for comparison	MD5	SHA256
Hash value	It can produce 128 bits of hash value.	It can produce 256 bits of hash value.
Attack required to find out original message	2^128 bits operation required to break.	2^160 bits operations required to break.
Speed	Faster, it required only 64 iterations.	Slower it requires 80 iterations.
Security	Poor security is provided.	Complex security is provided.
Successful attacks so far	Attacks reported to some extends	No such attach report yet.

Fig. 6. comparison between MD5 and SHA256

REFERENCES

[1] Ellewala, U. P., Amarasena, W. D. H. U., Lakmali, H. S., Senanayaka, L.M.K., Senarathne, A. N. (2020, December). Secure Messaging Plat- form Based onBlockchain In 2020 2nd International Conference onAdvancements in Comput-ing (ICAC) (Vol. 1, pp. 317-322). IEEE.
[2] Stearns, M. (2019). A Decentralized Approach to Messaging UsingBlockchain Technology (Doctoral dissertation, California State Univer- sity, Northridge)
[3] Singh, R., Chauhan, A. N. S., Tewari, H. (2022, June). Blockchainenabledend-to-end encryption for instant messaging appli- cations. In 2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM) (pp. 501-506). IEEE
[4] Ahmed, S., Biswas, M., Hasanuzzaman, M., Mahi, M. J. N., Islam, M. A., Chaki, S., Gaur, L. (2022, April). A Secured Peer-to-Peer MessagingSystem Based on Blockchain. In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 332-337). IEEE
[5] Wang, H., Yu, Y., Zhao, J., Wang, J. (2021, November). Blockchain-BasedTrusted Instant Messaging Model Research. In 2021 4th International Confer- ence on Hot Information-Centric Networking (HotICN) (pp. 32-37). IEEE
[6] Wang, H., Yu, Y., Zhao, J., Wang, J. (2021, November). Blockchain-Based Trusted Instant Messaging Model Research. In 2021 4th Interna- tional Confer- ence on Hot Information-Centric Networking (HotICN) (pp. 32- 37). IEEE
[7] Jia, C., Geng, Y., Sun, S. (2022, January). Research on Data Access Manage- ment Based on Blockchain Engine. In 2022 International Conference on Big Data, Information and Computer Network (BDICN) (pp. 465-468). IEEE
[8] Yusof, M. K., Usop, S. M., AmriAbidin, A. F. (2011). Designing a Secure Architecture for Private Instant Messenger Application. In Inter- national Confer- ence on Computer Science and Information Technology(ICCSIT'2011)
[9] Santiago, C., Lee, C. (2020, October). Accelerating message prop- agation in blockchain networks. In 2020 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 157-160). IEEE
[10] Abdulaziz, M., C ulha, D., Yazici, A. (2018, December). A decentralizedapplication for secure messaging in a trustless environment. In 2018 Interna- tional Congress on Big Data, Deep Learning and Fighting CyberTerrorism (IBIGDELFT) (pp. 1-5). IEEE
[11] C., Geng, Y., Sun, S. (2022, January). Research on Data Access Man- agement Based on Blockchain Engine. In 2022 International Conferenceon Big Data, Information and Computer Network (BDICN) (pp. 465- 468). IEEE. 32



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY