Secure communication using blockchain technology

.Dr.HENRY
Department of Computer Application
Jain Knowledge Campus,Bangalore
Jain (Deemed to be University)
Bangalore, India
Bangalore, India

Dr.JULIE
Assistant Professor
Department of Computer Application
Jain Knowledge Campus, Bangalore
Jain (Deemed to be University)

Abstract–In this era of ubiquitous social media and messaging applications, peoples are becoming increasingly aware of the information privacy related issues of applications. Major SMS applications are going towards end-to-end encryption process (E2EE) for providing privacy to the users. The current security is with different service provider for neglecting the E2EE integration into the system, which are having more vulnerabilities. The present method of E2EE is controlled by different service provider's servers, for decryption process. The keys will stored with providers for backup and restoration process. User are confidence in the privacy about their data while using this application. A public key infrastructure (PKI) can be implemented to overcome this issues, basically it comes with more cost for implementation.Which make difficulties for roll out on global scale. This paper explain about blockchain based E2EE frameworks which can solve many problems related vulnerabilities in modern SMS system for secure communications. Public/Private key will be generated by device while installation of application and ask for (MNO) mobile network operator for receiving digital certificate for storing into the public blockchain. Any person can search any of person's certificate from the application server, and can securely communicate with any one using forward encryption mechanism.

Keywords -: *Blockchain Technology,cryptography, Mobile Networking.*

I. INTRODUCTION

The blockchain is a system that is designed to make more dependable transitions. Essentially, blockchain technology aids in the gathering of information and relies on cryptography resistance as a solution. This blockchain will be able to provide secure communication in both networks and computer networks. Secure transactions are possible on the blockchain. All network users can agree to validate transactions in a safe manner before the transaction records can be updated. It was costly to modify or modify this. External hackers would have to obtain access to all machines in the network that hosts the blockchain in order to change the information stored at the current time, which is not requestable.

Cryptocurrency and bitcoin this are designed by non-recognized person referring alias Satoshi Nakamoto. Bitcoingenerateand shows the transactional for a blockchain.

A blockchain is essentially a fault-tolerant shared database for recording the public detailed ledger of every transaction that has occurred and sharing this information among all users in the network. Every transaction in an open ledger is governed by the requirements of a large number of users. As a result of applying a mix of cryptography and permission, this strategy will provide benefits for increasing data integrity. As a result, there is no way to exert control. Each and every block of the blockchain will store the data. A time stamp and a link to the holy block, as well as cryptographic security using various algorithms. As a result, it will be secured using public key infrastructure. It uses public and private key encryption, as well as a hash technique, to securely handle data and communicate messages. There is no control by a central authority to hold and store data in a distributed ledger, it removes every point of failure, and communication is based on itpeer-to-peer network design, and it inherits the decentralisation SMS charities. How do public blockchains genuinely overcome PKI bead issues. The information shared in blockchain is a history of all transactions ever made. The ledger, which is saved in several copies across a network of computers, is referred to as a node. So, every time a user submits a transaction, it is recorded in a ledger, where the nodes are the blocks that ensure the transaction is genuine. The transaction is stored in the blockchain's chained mechanism data structure. The next Time-Stamp will be recorded at the same time as the previous one. Any alterations would be prohibited.

Engineers and investors alike are interested in this technology since it allows anyone to make an essay transaction into a network with decentralised business potential and a variety of cryptocurrency. The public and private mechanisms are used in public key approaches. There will be no authority to hold and keep the data and information network or database, which will be in the point communication with decentralisation, and cryptography will be used for encryption into any king of mobile network or network system, as well as for data hiding between the server, app, and users in the mobile network.Our approach's main purpose is to safeguard connections between network elements. The proposed architecture involves using blockchain to verify a user's identity and establish trust amongst users in order to send secure messages. Every user must only communicate with other users whose identities have been verified by a smart contract, and all other interactions must be regarded as malevolent. Each user who wishes to communicate with others via the system must register their identity and public key and deposit it on the blockchain.Ethereum can be used to create such a system. Blockchain-based secure peer-to-peer communication. In this paper, we show how blockchain can be used to protect transactions between many users. Since the introduction of bit DNS, no solutions have been presented. Block stack’s performance is limited by bitcoin's underlying blockchain. Certcoin will continue to be the central authority and will use the Namecoin blockchain as a distributed record of domains and public keys. which causes two issues delay for the controller and security issues with Name coin’s mining that has been combined. A smart contract promises that traditional systems will be able to implement an agreement with the help of a trusted third party.The contract's details are saved in the blockchain, which is updated each time the contract is used. Before sending/receiving data from the network, the smart contract verifies the identity linked with the public key contained in the blockchain is correct. It examines the validity of the Time-Stamp. Finally, the smart contract checks the signature of the user. With the help of solidity, we can create smart contracts.

ii. LITERATURESURVEY

Sahai et al. [1] proposed an ABE system for identity-based encryption techniques. So basically, it has two variants: KP-ABE and CP-ABE encryption and decryption methods that are reliant on users' attributes. This was originally employed in cloud computing to help data owners overcome methods such as data security and data access control, with the cloud as the out reference.In cloud computing research, the technique of access control is being discussed. However, there is still room for improvement in fog computing. The research team has just completed work on access control issues in this field and has begun to implement ABE in the environment, with the goal of enabling fine-grained data access control while also ensuring data security.

Stojmenovicet al.[2] proposed illustrate the possibility of a man-in-the-middle attack in which the gateway is breached or posed as a fake for the alternative of multiple users into the network for in-between interaction of these several user connections for data security via networks for communicating.

Han et al. [3] proposed a measurement-based system to assist users in avoiding connecting to bogus access points Their method identifies the rogue AP by calculating the round-trip time between the end users and the DNA server.

Arwa et al.[4] proposed a fog communication security feature that is based on an encryption technique It uses a key-exchange protocol based on the CP-ABE algorithm to ensure authentic secret conversations among a larger number of fog nodes. This issue has not been widely addressed by researchers. Researchers have recently begun to employ blockchains to construct safe apps that benefit clients in a variety of professions or branches.

Christidiset al.[5]outlined the blockchain application sector for IoT. They looked at how a blockchain smart contract may be integrated into the IoT. The Internet of Things (IoT) refers to the sharing of real-time data for object-based objects over the internet using radio frequency identification and product electrical codes. Blockchain can be used in a variety of systems, including identity management and the Internet of Things. Using a peer-to-peer (P2P) network of computers and a protocol.

Kamanashiset al.[6]proposeda multi-purpose layer security approach for securing data transfer into smart city platforms using embedded blockchains and smart devices. The research team employs the blockchain concept as a common database for storing diverse data linked to smart cities, including traffic and location. These details must be shared throughout the many components of smart cities. In smart cities, the key issues with this method are scalability and reliability In, the author presented a blockchain-based approach for censusing dispersed information storage in order to facilitate data exchange in the Internet of Things. The fundamental goal of implementing blockchain for data storage was to provide data access control.

Hema and Kesavan.[7]has discussed e-healthcare-related information in today's environment. One of the most difficult tasks facing the healthcare industry is keeping medical data and information secure. Cryptographic algorithms based on elliptical curves that serve to secure aspects of security, such as secrecy and integrity. This will reduce overhead time in a variety of areas, including insider danger.

Tsai et al.[8] ECC, which requires a smaller key size than RSA, has been researched in depth.This study looks at an ECC integrated unit, a smart card, and a fixable device that helps with data and information transmission while retaining crucial data quality. Vijayakumar and colleagues developed an Internet of Things-based wearable device that captures patient medical data and sends encrypted SMS messages to medical devices.

Poonguzhaliet al.[9]the blockchain data format has been proposed, in which the data integrity has been preserved by which market the current data has been appended. The transaction information has been entered into nodes that are a member of the network. The major method in this study is divided into two sections. The first is that data is initially stored in the blockchain and then encrypted using the ECC. This improves the essential data's security. Jisha and Philip have underlined the importance of elliptical curve cryptography in RFID-based IoT in healthcare systems. Because it employs fewer keys than other asymmetric-key schemes, the ECC is lightweight.

Beraet al.[10]have developed a clever Blockchain Access Control system that is used to detect hackers in networked communication devices.Karuppiah and Gurunathan discussed the use of e-health apps to process the trivial and non-trivial connections between various sensor signals.To increase the security of these two principles, the information is stored in the cloud,which uses fish Encrypting methods.Cloud computing also provides many advantages, But have significant security risk.

Senthilkumaret al.[11.] the blockchain concept, according to him, may be utilised to maintain integrity, confidentiality, and authentication. Only approved users have access to the information or data included in the block, according to the basic method.Which ensures that sensitive information is kept private and secure.

Massodet al.[12] this paper described the method of security distributed environment of protected cloud for its interior structure. By applying these methods to a variety of topologies, this study provides information security addressing cloud extraction into data security.

Chaoyang et al.[13] he discussed the benefits of elliptical cure cryptographic algorithms and contrasted them with nonelliptical cure algorithms. This work concludes for elliptical cryptographic algorithms that primarily demand tiny bits and give effective data security protection.

Al Omar et al.[14]presented a healthcare-related blockchain, primarily Medi chain, with a public key based method. (i.e. elliptical curve cryptography (ECC)), which is used to encrypt private data over a secure channel, this study provides a security structure for the healthcare sector.

Liu J., Li X., Ye L.,[15]IEEE of global communications conferences (GLOBECOM) IEEE; 2. BPDS, which is for blockchain dependence of private preserving data transmission for electronic medical information. (Google Scholar).

Joneset al.[16] proposed a body of research which shows the SMS usages which makes a value contribution which teaches a facilitator or broker, which help for motivating of use of SMS Overwide education, this paper shows path way of SMS into education how to implement any usage of it.

iii. METHODOLOGY

The main purpose is to ensure that network connections are secure. The proposed architecture involves using blockchain to verify a user's identity and establish trust amongst users in order to send secure messages. Every user must only communicate with other users whose identities have been verified by a smart contract, and all other interactions must be regarded as malevolent. Each user who wishes to communicate with others via the system must register their identity and public key and deposit it on the blockchain.

Blockchain-Enabled for Instant Messaging This proposed blockchain-backed of mechanism which aims to provides an real accuracy without any disturbance of the sharing the secret keys including third parties like udo message (IM) server. This spans secure SMS transference across many entities such as phone network MNOs, blockchain nodes, and IM servers, as well as the ending and receiving of users into gadgets, are examples.We design use of a permissioned. Blockchain with various entities such as the MNOs and IM server. The main authorized to being written it the blockchain via which sticked for block of blockchain.

Registration and certificate generation When the user Alice generates a key using the sh1-256 technique, which includes a public key K and a private key, it represents an identity (ID), which is a hash of the public key. Alice will safely store the private key and, in response to requests, register her identity for the associated public key in the blockchain, which will then be confirmed and validated by the network. Each public key has a timestamp associated with it. The Alice sign information is transferred to the blockchain together with the accompanying private key. The certificates of Alice are then recorded on each blockchain, with the following pieces of information: Alice's ID into her public key, the validity of her public key, and a timestamp.

1. Bob will sent a transitions. The smart contract will get message from the user Bob.

2. This smart contract will check if Bob's ID is present in the blockchain or not. The intelligent after will read alice and Bob's records.

3. It looks for ID, If exists into block. The it terminated to true.

4. Once the public key validates the smart contract will check to the every unique ID of the transaction of Time-Stamp.

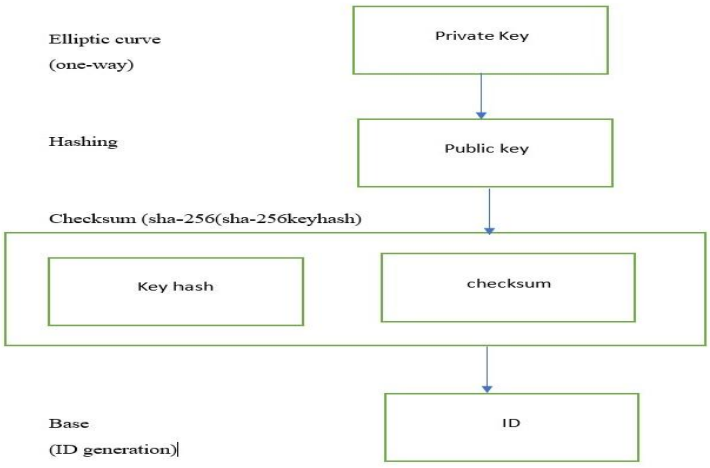

Fig-1 Key Generation

Sending /receiving a message Authentication will be established shortly after that. The allice will produce the secret using Bob's public key.To encrypt the message, the sheared secret will be produced using /elliptic-curve-duffle-Hellman.The ECDH algorithm encrypts communications and shares keys using an Elliptic-curve-Diffie-Hellman (EDCH) method. Data will also be encrypted using the symmetric key approach.

Smart Contract-Verifications On the blockchain, a smart contract is a piece of code that is saved and executed. After you've enabled the smart contract, the contract will be transmitted and validated without the ability for the user to amend or modify it. For transaction execution, a user can submit a transaction to a contact's address. As a result, every interaction will be recorded in the blockchain as a transaction. The transactions are organised into a Merkle tree, which is then stored in each block of the blockchain. When user Bob wants to send a message to Alice, Bob's ID will be saved on the blockchain, along with Alice's ID and the Time-Stamp. As a result, every message will carry a time stamp.

Android application using blockchain

Android is basically an mobile operating system which is originated from Linux kernel and other open source software, which is basically designed for touchscreen operating system. This platform uses the blockchain technology for secure transfer of mobile SMS service into the network with any kind of data leakage into the peer-to-peer communication. Make any easy for transmit the user date with help of blockchain into integrated smart contract code with specific aspect of block communication between several app users and without interaction of third party.

Reliability : As a result, moving all live charting room mobiles to blockchain is almost difficult because this database is always up and running.The smart contract code will work as expected once it is published. This is the primary benefit of their platform. The system ensures a secure movement within the SMS network by encrypting messages with blockchain technology and integrating them into various Android applications.

Confidentiality : The channel of communication between different users is mentioned as being highly secured with blockchain technology into the Android operating system, This makes it possible Peer-to-peer encryption between endpoints will be available only to authorised users. Users can use the software to send and receive messages on their mobile devices.

Message integrity : The blockchain will check for the valid user / signature, before the data stored into block. No third party person cannot change or modified the data into block the data is stored. On the blockchain, each user has a certificate. The certificate will be validated by the smart contract, and users' IDs will have access to it. All data exchange in the network is done using the ECDSA technique and a private key associated with a public key.

Fig.3Encryption analyses

This represent the AES encryption time, and MAC time as will, the total encryption time and in seconds to words string input up to 10,000 char using data transmit from hegraph, the average time took for AES encryption up to 576.509, and MAC was 1325.889, which shows the encryption of AES in CBC mode.

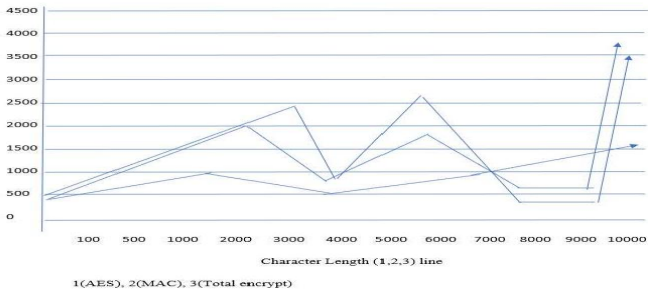

Fig.4Decryption analyses

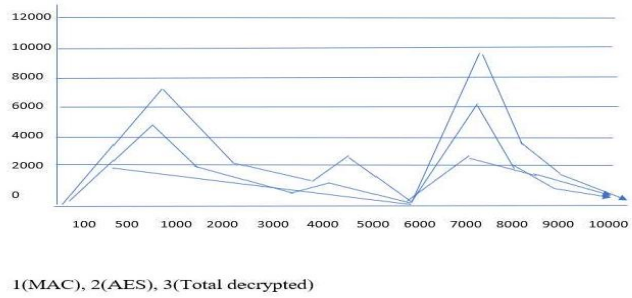

fig.3 how the graph for the decryption process of analysis time for calculating the AES-CBC decrypt time. The time analyses f AES is between 1689.134. as the average time was 3067.224 micro-sec gape. The result will how the Av length a large extent with rise in the character lengths.

IV. CONCULUSION

This research looked at the state-of-the-art benefits of a decentralised architecture with built-in fault tolerance, redundancy, and transparency. This research created a mechanism for

securing data transfer between Android mobile devices and addressing high challenges in the realm of centralised PKI.We intend to implement depending on the results of the proposal and the functionality of the Android application. Our next suggestion is to create an architecture with a smart contract to validate certificate input and revocation on a public blockchain. Which will contain the public key, as well as the address of the smart contract that is stored in it and off-chain.

V. REFERENCES

1. Sahai et al, research papers for identity-based encryption algorithms . KP-ABE and CP-ABE encryption and decryption methods used in cloud(fuzzy identity-Based encryption research module)

2. Stojmenovic et al, a detection and prevention methods man in middle attack in fog computing www.sciencedirect.com research article.

3. Han et al, (2017_H. Han, B. sheng, C. Tan, Q, Li, " A measurement based rogue access point detection scheme ,INFOCOM,2009,pp.1593-1601.

4. Arwa et al, An attribute based encryption scheme to secure fog communication (2017) may. IEEE Access PP(99):1-1 D(10.1109/Access.2017.2705076).

5. Christidis et al, telematics informatics vol-36 (2019) a systematic literature review of blockchain based applications.

6. Kamanashis et al, multi-layer blockchain-based security architecture for internet of things (10.3390/s21030772) IoT and D2D researchgate.net.

7. Hema and Kesavan, security and privacy challenges of cryptography applications in e-health security systems. (IEEE) .ieee.org.

8. RSA algorithm academia.edu (Implementation of RSA algorithm using Mersenne prime).

9. Poonguzhali et al, blockchain enabled IoT and sensor technology in wireless networks (hindawi.com) security communication network.

10. Bera et al, designing blockchain based access control protocol in IoT enabled smart grid system (IEEE internet of things journal) PP(99):1-1 10.1109/JIOT.2020.303008.

11. Secure authentication and integrity techniques for randomized secured routing in WN (10.1007/s11276-014-0792-0).

12. A review of machine learning algorithm for cloud computing security mdpi.com. Electronics 1379.

13. Chaoyang et al, survey of elliptic cure cryptosystem, (ECC) research paper.by SC vo. Part-1

14. Al Omar et al, privacy friendly platform for healthcare data in cloud based on blockchain environment (D 10.1016/j.future.201812.044) researchgate.net.

15. A survey on blockchain system: attacks, defences and privacy preservation. (sciencedirect.com).

16. Jones et al,SMS communication support and enhance. Research in learning technology.(3) 10.3402/jrlt.v17i3.10887.Rearchgate.net.