International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1292-1298 www.ijaem.net
ISSN: 2395-5252

Blockchain Based Data Security for Fog Enabled IoT Infrastructure

L A Nithya Shree, Dr. Rajendra R Patil
Dept, of ECE, GSSSIETW Mysuru, Karnataka, India
Professor and Head, Dept, of ECE, GSSSIETW Mysuru, Karnataka, India

Submitted: 10-07-2022 Revised: 18-07-2022 Accepted: 23-07-2022

ABSTRACT - Fog computing is a brand-new skill that works in conjunction with the cloud tobring its services near to the user's gadgets.
Cloud is often situated far from the strategies that use its services. In order to support evidence-based decision making in companies and governments, data security is crucial. The Internet of Things (IoT) devices and systems, for example in a fog environment, are one of the important data sources. The intricacy and interconnectedness of such IoT and fog environments, however, can lead to security weaknesses which can be used to undermine the validity of the data. For fog computing to operate properly, security is a key component. In fog computing, key exchange must be taken into account. Since fog servers offer facilities to several users, guaranteeing secure mutual validation is crucial for the safety of fog computing. In order to guarantee the security of data transmission in the fog environment, we suggest a safe Blockchain-based scheme in this paper.
Keywords- Fog computing, IoT, Blockchain

I. INTRODUCTION

In the Internet of Things (IoT) paradigm, the FOG environment can be seen as a transitional architecture between the terminal nodes of the physical layer and the user devices. Although the terms "fog computing" and "edge computing" are frequently used synonymously in the media, the two concepts have a few subtle differences [1]. To compute, store, and provide online services, the former (fog computing) can be thought of as a platform that is highly virtualized between cloud data centres and terminal installations [2]. No framework is great, and comparably, there are a number of difficulties related with fog conditions. For instance, how would we productively and successfully verify the fog hubs, taking into account their variety of equipment and programming, found at various control layers,[3] and additionally distinguish (possibly) pernicious information that are on the way between various fog conditions [4][5], for instance, because of man-in-the-middle and different assault [6]. Almadhoun R in [7] have proposed a Blockchain system and implemented the same using Ethereum platform and smart contracts for IoT devices validation in a decentralized manner with no third party intervene. They implemented the proposed system using solidity language. IoT devices authenticating at large scale is featured by involving fog nodes are used to free IoT devices from the processing demands of handling authentication activities and the connectivity costs associated with interacting with the Ethereum Blockchain network. Patwary in [8] have proposed new authentication technique that was necessary for the Fog environment to be secure. They suggested a distributed (decentralised) method of area-based Device to Device confirmation that is made for Fogdevices at the Fog layer and is independent of any intermediary, trusted third party. They used Ethereum smart contracts in conjunction with blockchain for implementing the common validation mechanism. Only for authentication purposes, the Fog devices must keep keys. Therefore, the suggested technique demonstrated that authentication method was resistant to common cyberattacks and satisfied security needs. Fotohi, Rproposes a two technique. In the first technique using blockchain they authenticate each link using the identity-based signature for safe interaction among devices. Second method is that blocks are shown by hashing. The conceptual analysis and simulation results showed that the suggested method outperformed S-LoRaWAN and DLBA-IoT in terms of average sensitivity, bit rate, reliability, idle away time for node validation, and energy used to

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1292-1298 www.ijaem.net
ISSN: 2395-5252

perform an action. The simulation results also demonstrate how the suggested technique can dramatically increase network security. Khalid U in have proposed a system without centralised authentication and allow portable IoT devices to manage who is authorized to access data and resources. This mechanism can be used in a wide range of applications. The technique used a public blockchain concept and fogging. The experiment's findings show that the suggested mechanism

outperforms a state-of-the-art blockchain-based authentication method in terms of performance. Eric Pardede [11] proposed a fog-based mutual authentication technique that makes use of low-cost primitives like hash functions and elliptic curve cryptography (ECC). To ensure that their authentication strategy defends end users against various attacks, they validate it using the security protocol animator of automated validation of internet security protocols tool. Their system offers a safe and mutual key exchange protocol between three parties the cloud, fog, and edge devices. Otuekong Umoren in [12] proposes an authentication system by utilizing blockchain and transaction protocol which is a program that run when the conditions are met to validate operators safely. The implemented system registers and authenticates users using their electronic mail address, username, Ethereum platform address, PIN, and information from a biometric reader. Desire Ngabo in [13] focus to find ways to reduce problems with the fog computing architecture's latency, security, centralization, and scalability. They used elliptic curve cryptography digital signature as a hash function with a public-permitted blockchain. This security mechanism offers a permanent safety result for medical information in IoT fog layer. File with the hash code with the sharing link is encoded and a credential is supplied that can only be opened by the intended requester in the case when anybody can request the files. The detected data was also recorded in a database where blockchain is used and a copy of the data is processed to a cloud record where it used as another fogs. Mohammed Alshehri in [14] proposes an algorithm which will allow owner of the data to share encrypted data only with user who is approved and also proposed new technology known as blockchain used for a data access control method to protect data of user from malicious fog nodes in the event that a conceded fog node is removed. With this strategy they suggested groups of fog nodes with similar services and geographic regions. Marco Conoscenti [15] determines whether a decentralised and private-by-design IoT may be fostered using peer-to-peer and blockchain technologies. As the first phase they conducted a Literature Review on the blockchain to acquire information on the present applications of this technology and to document its current level of integrity, anonymity, and flexibility. Chan Hyeok Lee [16] proposes system which uses Zero-knowledge proof and smart contract to protect data. To stop internet of things device verification and information altering, information is kept in the blockchain. They proposed a system to protect user original data from viewing from the intruders by using Zero-knowledge proof technology is. Mobius IoT open server platform is used to implement a system that can share data from device to application and it is used to upload it to block chain server. Jin Hyeong Jeon [17] proposed blockchain based a new IoT server platform to store data in blockchain. Real-time sensor data is collected by the IoT server platform chosen by Mobius, which is then managed and stored in a MySQL database. The Mobius configuration of MySQL, however, has a number of security flaws and risks. Instead of using a generic server method like MySQL server, they proposed a data storing method by creating the blockchain as a folder which contains database. Blockchain technology along with IoT improved safety and they utilized Smart Contract. Ethereum blockchain encoding technique and validation technique were used. Hittu Garg [18] proposed a system to safeguards the complex information is not visible to every user using an algorithm which will allow owner of the data to share encrypted data only with user who is approved as an admission controller mechanism at middleware. System proposed guarantees data security and privacy while giving users the freedom to specify which information is permitted for user to access. There are a few security vulnerabilities with CP-ABE schemes, including forward and backward security issues. Additionally, access to sensitive data is controlled by a centralised authority, which raises additional security challenges. Trusit Shah [19] proposed mutual authentication system that is multi-password based. This method uses a secure vault, which is a set of keys of similar sizes and that is shared secret between the IoT server and the IoT device. The secure vault's initial contents are shared between the server and the IoT device, and next they are updated after each successful communication session. Arduino microcontroller was used to build this method and to demonstrate that algorithm works on IoT devices with limited memory and processing

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1292-1298 www.ijaem.net
ISSN: 2395-5252

capacity. Guy Zyskind [20] Personal and sensitive information should not be hand overed to third-parties because they could be attacked or used inappropriately. Instead, people should be in charge of and own their data without sacrificing security or impeding businesses' and governments' abilities to offer specialised services. Their architecture makes this possible by fusing an off-blockchain storage solution with a blockchain that has been repurposed as an access-control moderator. Users are always informed of the information that is being gathered about them and how it is used, and they are not obliged to put their trust in any third party. The blockchain also acknowledges consumers as the true proprietors of their personal data. Anthony Lo in proposed multicast verification schemes for smart grid communications which are TVHORS and TSV. A thorough comparison of TV-HORS with TSV+ reveals that, at the sacrifice of signature size, TV-HORS offers much more efficient signing and verification for the same security level. Arij Ben Amor in [22] provide a user using fog and server of the fog a two-way authentication system whereby a user and a server validate one another to create a key for a session without revealing the user's true individuality. Elliptic Curve Discrete Logarithm Problem, pseudonym-based cryptography, and bilinear pairing are foundations of their system to establish the session key. Automated validation of internet security protocols tool is used for security examination and to test a proper authentication is done. In our work our objective is to secure user's data by creating a block with hash code using blockchain technology. To generate keys and to create block for each key in fog environment. To recover the keys or data if tempered.

II. PRELIMINARIES

Here we will introduce necessary concepts required to build system. Firstly, we will explain about fog computing, blockchain and algorithms.

A. Fog Computing

Cisco is credited for creating the phrase fog computing. It is a cutting-edge technology with numerous advantages, particularly for the Internet of Things. Fog computing offers IoT customers capabilities like data processing and storage, just like the cloud does. Fog computing is centred on giving fog devices access to data processing and storage on-site rather than transferring it to the cloud. These devices are referred to as Fog nodes. Anywhere with a network connection can use them. Fog nodes can be any tool which have estimating capacity, storing capacity, and web connectivity, along with embedded servers, manufacturing controllers, hub, modem, and security cameras. Fog and the cloud both offer networking, computation, and storage resources. Fog computing is used in the Internet of Things (IoT) to increase performance, efficiency, and to transport less data to the cloud for processing, analysis, and storage. As a result, network edge devices will receive and interpret the data that sensors have collected.

B. Blockchain technology

A Blockchain Technology is a digital ledger of communication or transaction where every transaction is duplicated and distributed across a network. It is distributed immutably. By utilizing this innovation, it is challenging to hack or change any information in the record. Each block in a chain contains various exchanges. Whenever another exchange is being made in the blockchain network then that exchange is enrolled on each client's record on the organization. It really intends that on the off chance that a solitary block is controlled in a chain, it will come into notice effectively that it is changed. If somebody has any desire to change or control anything in a block then they ought to control each block over the disseminated network. Whenever a new transaction is being made in the blockchain network then that transaction is registered on every user's ledger on the network. Blockchain is a decentralized architecture hence it needs a decentralized preservation, saving the data in a blockchain is easy, transportation of data in a secure manner, data access is simple with anti-tampering features and high level of data security. Blockchain consists of three important things: blocks, nodes and miners.

C. AES algorithm for encryption and decryption of data

Data can be concealed using the 128-bit, 192-bit, or 256-bit Advanced Encryption Standard (AES) technique. One secret key is used by the AES algorithm for both encryption and decryption. The AES algorithm is shown in picture 3.6. A secret key is used to encrypt and transform plain text into cipher text before it is sent from the sender to the recipient. The recipient's end uses the same secret key for decryption in order to translate the cipher text into plain text.

III. METHODLOGY

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1292-1298 www.ijaem.net
ISSN: 2395-5252

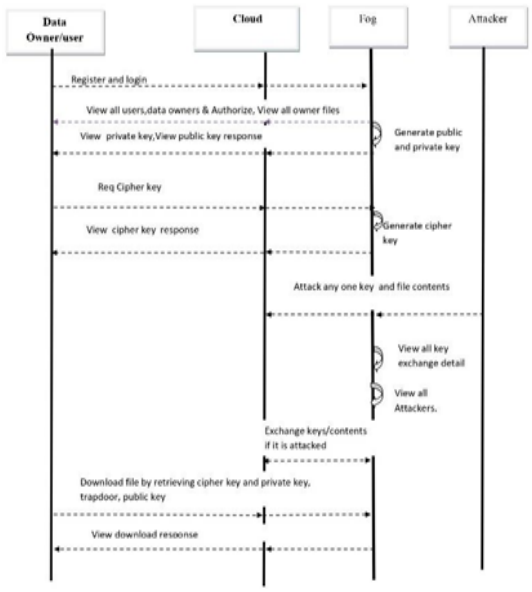

Fig 1: Proposed system

To overcome the security and privacy issues arising in the Fog computing, blockchain system is designed for securing files by using Advanced encryption standard to encrypt and decrypt the data files and Blockchain technology for storage. Figure 1. shows the proposed system architecture. Web based application designed using J2EE technology with Tomcat as web server and MySQL as database server. Cloud is used for storage purpose. All the files of data owner are stored. If key is tampered then key exchange can take place between fog and cloud. Fog is used to generate keys. Data owner can uploadfile and verify files.

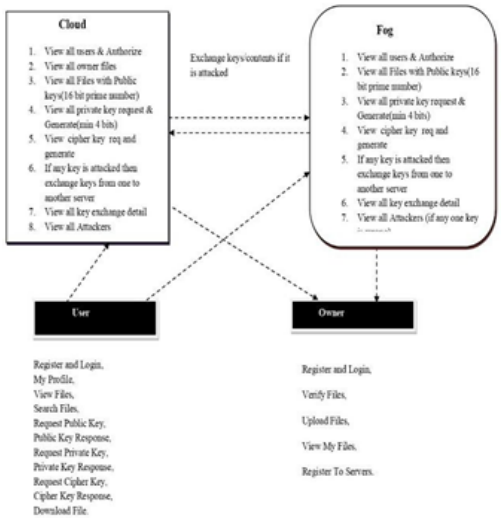

Fig 2: System architecture

Figure 2 shows system architecture. In this module the Cloud and fog will authorize users and view all the files uploaded by user with the public key, view all the private key request and generate the key and view the same, view all the cipher key request and generate the key, if either of the key is attacked by the attacker the keys will be recovered from the other server and view the key exchange details and attackers who attacked the keys. End User has to register to both the servers and get authorized to login, if not registered with either of the server it will prompt to register with corresponding server, once logged in the user will request data from the cloud, the user has to request for public key, private key and cipher key and view the same response, verify the file and exchange the file from other server if the file is attacked and changed its contents. Similarly download the file by giving public, private and the cipher key. In this module, Data owner has to register to both the servers to login, if not registeredwith either of the server it will prompt to register with corresponding server, once logged in the user will browse for files encrypt and upload it with the public key and store in Cloud server and performs the following operations such as Verify Files, Upload Files, View My Files, Register to Servers. Data is encrypted using AES algorithm, public key is generated using RSA algorithm and SHA1 is used as hashing algorithm.

IV. RESULTS

Results shows how the blockchain based System aweb-based application helps in solving the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1292-1298 www.ijaem.net
ISSN: 2395-5252

privacy and security issues raised by using traditional database storage. The result of using blockchain and AES based encryption is discussed.

Fig 3 : Home Page of the system

Figure 3 shows home page of blockchain based system for fog enabled IoT infrastructure where it displays the name of the project and concept of the project. Different members of the system are mentioned at the top. By clicking on any one of the members it will direct to the home page of that member.

Fig 4: Home page of Cloud server

Figure 4 shows the cloud server home page where a welcome is displayed after the cloud login and concept is also displayed. At the left of the home page there are several tabs such as, view users,owner files, files with public key and log out. Cloudserver act as a storage system.

Fig 5: Home page of fog

Figure 5 shows the fog server home page where a welcome is displayed after the fog login and concept is also displayed. At the left of the home page thereare several tabs such as, view users, files with public key, public key permission, generate private key, generate cipher key, and log out. Fog server is mainly use to generate keys.

Fig 6: Home page of data owner

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1292-1298 www.ijaem.net
ISSN: 2395-5252

Figure 6 shows home page of data owner where a welcome is displayed after the data owner login and concept is also displayed. At the left of the home page there are several tabs such as, upload files, verify files, view my files, register to server and logout.

Fig 7: Data owner uploading file page

Figure 7 shows encrypted file and the hash code generated and data owner can upload the file.

Fig 8: End user home page

Figure 5.15 shows the end user home page along with welcome page and concept of the project. At left side there will be menu like my profile, view files, request public key, public key response, download file and various other menu.

Fig 9: Key exchange details

Figure 9 shows key exchange detail in fog server. It will have record of both new and old keys. New key means the key edited by the attacker

V. CONCLUSION

Web based Application is designed for fog enabled IoT infrastructure to maintain the security of data using Blockchain. File is encrypted using advanced standard encryption. Encrypted file and hash code will be in block. Public key, private key and cipher key will have maintained in a block. Since all the data is maintained in blockchain security can be achieved. Future work includes different data files like Images, Videos can be implemented. IoT devices can be implemented to generate data.

ACKNOWLEDGMENT

I would like to thank our Principal, Dr. M Shivakumar. Dr. Rajendra R Patil, my guide and Head of ECE GSSSIETW Mysuru for his support for completing my work also I thank my PG coordinator Dr. Shyamala C for her continuous support. I also thank DST-CURIE for their support and for providing financial assistance to publish

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1292-1298 www.ijaem.net
ISSN: 2395-5252

this paper.

REFERENCES

[1] F. Aït-Salaht, F. Desprez, and A. Lebre, (2020). An overview of service placement problem in fog and edge computing, ACM Comput. Surveys, vol. 53, no. 3, pp. 1–35.

[2] F. Bonomi, R. A. Milito, J. Zhu, and S. Addepalli, (2012). Fog computing and its role in the Internet of Things," in Proc. 1st Ed. MCC Workshop Mobile CloudComput., pp. 13–16.

[3] Z. Hao, E. Novak, S. Yi, and Q. Li, "Challenges and software architecture for fog computing," IEEE Internet Comput., vol. 21, no. 2, pp. 44–53, Mar./Apr. 2017.

[4] K. Hong, D. J. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the Internet of Things," in Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput., 2013, pp. 15–20.

[5] L. Zhang, W. Jia, S. Wen, and D. Yao, "A man-in-the-middle attack on 3G-WLAN interworking," in Proc. IE

[6] W. Liang, W. Huang, J. Long, K. Zhang, K.-C. Li, and D. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," IEEE Internet Things J., vol. 7, no. 7, pp. 6392–6401, Jul. 2020.

[7] Randa Almadhoun, Maha Kadadha, Maya Alhemeiri (2018). A user authentication scheme of IoT devices using blockchain-enabled fog nodes. IEEE, 1-8.

[8] Abdullah Al-Noman Patwary, Anmin Fu, Sudheer Kumar Battula (2020). FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain. Elsevier, 162, 212–224.

[9] Reza Fotohi, Fereidoon Shams Aliee (2021). Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. Elsevier, 197, 108331.

[10] Umair Khalid ,Muhammad Asim, Patrick C. K. Hung, (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Springer, 23, 2067–2087.

[11] Rudri Kalaria, A.S.M.Kayes, EricPardede (2021). A Secure Mutual authentication approach to fog computing environment. Springer, 111, 102483.

[12] Otuekong Umoren, Raman Singh, Zeeshan Pervez (2022). Securing fog computing with a decentralised user authentication approach based on blockchain. MDPI, 22, 3956.

[13] Desire Ngabo, Dong Wang, CelestineIwendi (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of Internet of Things. MDPI, 10, 2110.

[14] Mohammed Alshehri, Brajendra Panda, Sultan Almakdi (2021). A NovelBlockchain-based encryption model to protect fog nodes from behaviors of Malicious Nodes. MDPI, 10, 3135.

[15] Marco Conoscenti, Antonio Vetro, Juan Carlos De Martin (2016). Blockchain for the Internet of Things: a Systematic Literature Review. IEEE, 978-1-5090- 4320.

[16] Chan Hyeok Lee, Ki-Hyung Kim (2018). Implementation of IoT System using BlockChain with Authentication and Data Protection. IEEE, 978-1-5386-2290-2.

[17] Jin Hyeong Jeon, Ki-Hyung Kim, Jai-Hoon Kim (2018). Blockchain based data security enhanced IoT Server Platform. IEEE, 978-1-5386-2290-2.

[18] Hittu Garg, Mayank Dave (2019). Securing user access at IoT middleware using attribute-based access control. IEEE,45670.

[19] Trusit Shah, S. Venkatesan (2018). Authentication of IoT device and IoT server using secure vaults. IEEE, 2324-9013.

[20] Guy Zyskind, Oz Nathan, Alex Sandy Pentland (2015). Decentralizing privacy: using blockchain to protect personal data. IEEE, 181-184.

[21] Anthony Lo, Yee Wei Law, Marimuthu Palaniswami, Gina Kounga (2013). WAKE: Key management scheme for wide-area measurement systems in smart grid. IEEE, 0163-6804.

[22] Arij Ben Amor, Mohamed Abid, Aref Meddeb (2017). A privacy-preserving authentication scheme in an edge-fog environment. IEEE, 1225-1231.