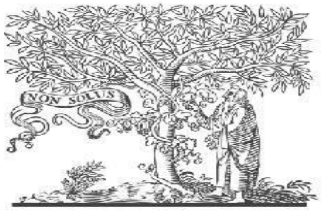
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 05th Apr 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/140

Title DECENTRALIZATION AND SECURITY ISSUES IN BLOCKCHAIN ENABLED INTERNET OF THINGS

Volume 12, ISSUE 04, Pages: 1092-1097

Paper Authors

G Shriya, Panjala Divya, Vadla Vani , Voruganti Naresh Kumar

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DECENTRALIZATION AND SECURITY ISSUES IN BLOCKCHAIN ENABLED INTERNET OF THINGS

G Shriya[1], Panjala Divya[2], Vadla Vani[3], Voruganti Naresh Kumar[4]

[1]B. Tech Student(IV), Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, gshriya1225@gmail.com

[2]B. Tech Student(IV), Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, divyapanjala26@gmail.com

[3]B. Tech Student(IV), Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, vadlavani5731@gmail.com

[4]Associate Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India, nareshkumar99890@gmail.com

ABSTRACT: This article discusses security concerns for patient health records stored on a Blockchain server that is decentralized (data will be maintained by various peers or systems). Multiple hospitals, insurance companies, the government, and laboratories can now share patient data. Patients will face data security risks as a result of data sharing because agency employees may misuse or steal the data. The author is making use of a Decentralized Blockchain server to deal with this problem. This server stores data as blocks of trees and verifies previous hash codes at each transaction; assuming check is effective, the information is thought of as unblemished; The Blockchain server notifies the system that it is under attack and collects data from another functioning node if data changes. Blockchain is secure and reliable in today's market due to its immutable data storage and transaction hash code verification. Creator is utilizing encryption strategies prior to placing information in Blockchain to more readily shield information, and writer has depicted a few old and novel encryption calculations like ABE, IBE, CPABE, and some more. I am using the AES method to encrypt patient data prior to storage because Python does not yet support the ABE algorithm.

Keywords *– AES algorithm, blockchain, Encryption, Decentralization*

1. INTRODUCTION

The Internet of Things (IoT) addresses one of the vitally dangerous progressions of this truly significant stretch. It is a characteristic movement from the Internet (of PCs) to implanted and cyber physical frameworks, or "things" that seem as though PCs yet really contain PCs. Data about our reality and climate can be gathered at a lot higher granularity utilizing an organization of reasonable sensors and interconnected objects. As a matter of fact, such top to bottom information will increment efficiency and offer state of the art types of assistance in an extensive variety of use spaces, including savvy city administrations and ubiquitous medical care. In any case, serious protection and security concerns emerge because of the undeniably thick, undetectable, and unavoidable assortment, handling, and dispersal of information in the confidential existences of people. From one viewpoint, this information can be utilized to furnish clients with an assortment of helpful, refined, and individualized administrations. Then again, data that can be utilized to algorithmically make a virtual memoir of our exercises and uncover private way of behaving and way of life designs is implanted in this information. The absence of central security shields in a large number of the original IoT items at present accessible available worsens the protection gambles related with IoT. Vehicles and brilliant locks, among other associated gadgets, have been found to have various security blemishes. IoT's intrinsic security and protection issues are exacerbated by the accompanying: scale, setting mindful and situational nature of dangers, heterogeneity in gadget assets, different assault surfaces, and absence of focal control

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

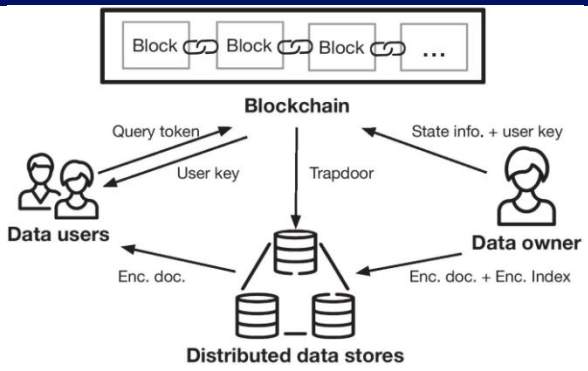


Fig.1: Example figure

As a result, IoT privacy and security are receiving a lot of attention from researchers. A conveyed capacity based admittance control framework is introduced to control admittance to delicate information. Be that as it may, their proposed arrangement might think twice about security and incorporates pointless postponements and expenses. The creators utilized IPsec and TLS to empower validation and security, however both are computationally costly and may not be appropriate for the majority IoT gadgets with restricted assets. Introduced a protection the board framework looks at the gamble of uncovering information to other people; nonetheless, generally speaking, the obvious advantage of IoT organizations counterbalances the bet of safety disaster. In this way, there is a necessity for security careful IoT data exchange that doesn't endanger client insurance. In conclusion, these and other previous efforts to guarantee IoT privacy and security have not yet addressed all of the aforementioned issues.

2. LITERATURE REVIEW

BlendCAC: A BLockchain-Enabled Decentralized Capability-Based Access Control for IoTs

Heterogeneous inserted savvy gadgets can now team up to make shrewd administrations regardless of human cooperation because of the far and wide utilization of the Internet of Things (IoT). Regardless of the way that exploiting colossal extension IoT-based applications, for instance, Clever Support or Splendid Metropolitan regions, IoT furthermore raises assurance and security issues. One of the fundamental security gives that the Web of Things faces is access approval, which is fundamental for sharing assets and safeguarding data. One of the ongoing access control (AC) blemishes is the brought together approval server, which might be a presentation bottleneck or a weak link. This article depicts BlendCAC, a blockchain-empowered decentralized capacity based AC for IoT security[1]. In enormous scope IoT organizations, the BlendCAC means to give viable access control systems to gadgets, administrations, and information. For the dissemination of access consents, a limit designation framework in light of the blockchain network is proposed. A brilliant agreement is utilized to enroll, spread, and renounce access approval in a complete character based capacity token administration framework. Instead of being coordinated by a united power, IoT gadgets are their own master under the organized BlendCAC thought. The trial results, which were executed and assessed on a Raspberry Pi gadget and a little private blockchain network, show that the proposed BlendCAC strategy can be utilized to give IoT frameworks an air conditioner arrangement that is decentralized, versatile, lightweight, and fine-grained.

Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT:

The Internet of Things (IoT) is developing and laying down a good foundation for itself as a part of the Internet of Things representing things to come. One of the innovative impediments is the ability to oversee billions of worldwide gadgets. There are apparatuses for overseeing IoT access, however they depend on incorporated models, which presents new innovative imperatives while overseeing them all around the world[2]. For the Internet of Things, we propose an original engineering for settling jobs and consents. The new designing is a blockchain-based completely dispersed induction control framework for IoT. The plan is upheld by a proof of idea execution and has been tried in certifiable IoT applications. According to the findings, blockchain technology has the potential to be utilized as a tool for access management[3], particularly in scalable IoT scenarios.

A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions:

The Internet of Things (IoT) is developing and turning into a piece representing things to come Internet. The capacity to control billions of gadgets

across the globe is one of the innovative hindrances[4]. Access the board apparatuses exist in the Internet of Things, however they depend on unified models, which presents new mechanical limitations while overseeing them universally. We present an original design in light of blockchain innovation for settling jobs and consents in the Internet of Things, which is a disseminated admittance control framework. A proof-of-idea execution and real IoT applications have been utilized to test the design. The discoveries propose that in some versatile IoT situations, blockchain innovation could be utilized as an entrance the executives device.

Blockchain-Enabled Edge Intelligence for IoT: Background, Emerging Trends and Open Issue:

A collection of entries with sequential time stamps is referred to as the blockchain in the distributed ledger technology (DLT) category. This method of decentralization has developed into an effective model for establishing verifiable trust among untrustworthy parties. Because of ongoing headways in multi-access edge computing (MEC) and artificial intelligence (AI), blockchain-empowered edge knowledge has arisen as an arising innovation for the Internet of Things (IoT)[5]. New examples are found, as are unanswered examination questions, as we research how blockchain-empowered edge knowledge works in the IoT. More specifically, (1) we give a comprehension of DLT, MEC, and simulated intelligence on a crucial level; (2) To distinguish arising patterns in this study field, we give a complete examination of the latest writing checked on by peer survey; (3) We cause to notice a few unanswered inquiries and exploration holes that ought to be filled from here on out. We expect blockchain-engaged edge understanding to be a basic facilitator of future IoT, enabling trust and information to fulfill the puzzling requirements of associations and society.

3. METHODOLOGY

We use a normalization database in our current system, which is easy to manipulate in terms of patient data. Data storage, privacy, and security have all emerged as significant issues for IoT devices. Scaling to meet the needs of future IoT systems is difficult due to the centralized design approach used in current systems. The study of blockchain has emerged as a promising area for dealing with the aforementioned problems. The distributed database system known as blockchain is capable of storing all transaction data. Without relying on central players, it can provide the necessary security and dependability in an untrustworthy environment. Blockchain will allow IoT devices to submit data to the blockchain ledger in order to prevent manipulation and counterfeiting.

Disadvantages:

1. Patients will face data security risks as a result of data sharing because agency employees may misuse or steal the data.
2. It is necessary for the system to be properly computerized in order to get around all of these limitations and make its operation more accurate.

Decentralized blockchain server that verifies previous hash codes at each transaction and stores data as blocks of trees; assuming check is effective, the information is thought of as unblemished; The Blockchain server notifies the system that it is under attack and collects data from another functioning node if data changes.

Blockchain is secure and reliable in today's market due to its immutable data storage and transaction hash code verification. Creator is utilizing encryption strategies prior to placing information in Blockchain to more readily shield information, and writer has depicted a few old and novel encryption calculations like ABE, IBE, CPABE, and some more. I am using the AES method to encrypt patient data prior to storage because Python does not yet support the ABE algorithm.

Advantages:

1. At the point when information changes, the Blockchain server tells the framework that it is under attack and accumulates information from another utilitarian hub.
2. All previous hash codes are verified during each transaction, and if the verification is successful, the data is regarded as intact.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

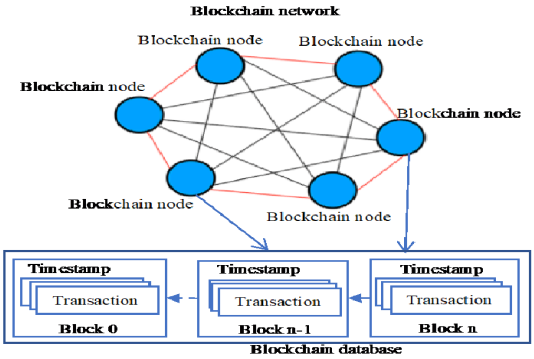


Fig.2: System architecture

MODULES:

The users listed below may carry out this project.

1) Users: These are patients who provide Healthcare agents with access to their medical profiles; An access control software can be used to control this access and decide which users are allowed to view patient data.

2) Providers of Healthcare: Patients' data can be accessed by the government to determine the prevalence of specific diseases, which can be done by physicians, insurance companies, or government users. This data can be used by doctors to treat patients and insurance companies can use it to decide whether or not to provide insurance to patients.

3) Cloud Data Backup: We will consider Blockchain-encrypted data storage to be cloud storage because we do not have a cloud server.

4. IMPLEMENTATION

Blockchain Hash Function:

An information string (numbers, letter sets, or media records) of any length is changed into a line of a foreordained length utilizing a hash capability. Contingent upon the hash calculation utilized, the decent piece length might differ (for instance, 32 pieces, 64 pieces, 128 pieces, or 256 pieces). A hash is the result with a proper length. This hash is likewise the cryptographic result of a hash calculation. The outline underneath assists us with understanding.

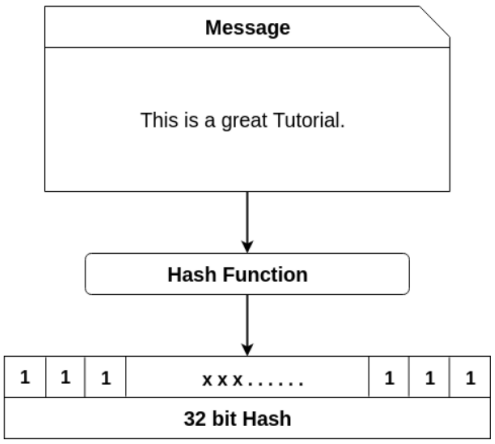


Fig.3: Blockchain hash function

The qualities of the hash calculation are as per the following: It delivers a one of a kind result, otherwise called a hash. There is just a single way it very well may be utilized. The blockchain's agreement cycle utilizes the qualities of this cryptographic hash capability with regards to digital forms of money like Bitcoin. An overview, or computerized finger impression, of a bunch of information is a cryptographic hash. Cryptographic hash capabilities accept exchanges as information and cycle them through a hashing interaction to create a fixed-size yield.

The resulting hash cannot be used to retrieve the entire text because the Hash function is one-way. This contrasts from standard cryptographic activities, for example, encryption, in which you might scramble something utilizing the key and afterward translate the message to its unique structure utilizing decoding.

5. EXPERIMENTAL RESULTS

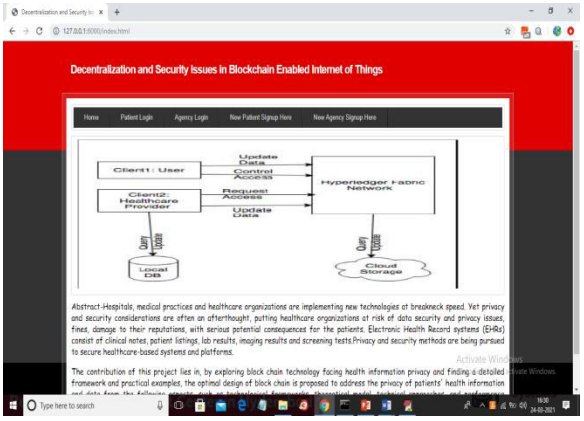


Fig.4: New user signup here

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

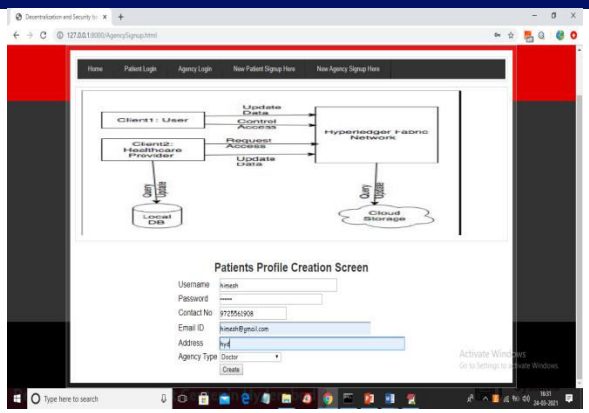


Fig.5: Patient profile creation screen

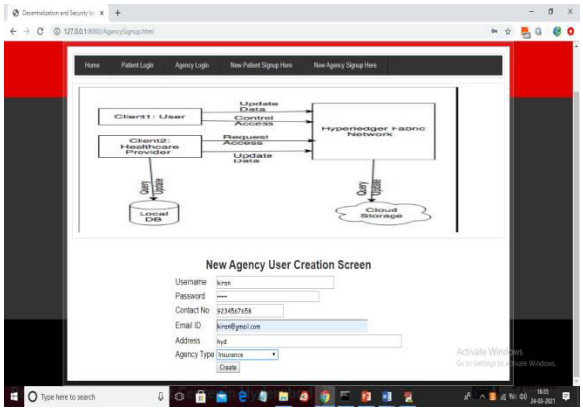


Fig.6: New agency creation screen

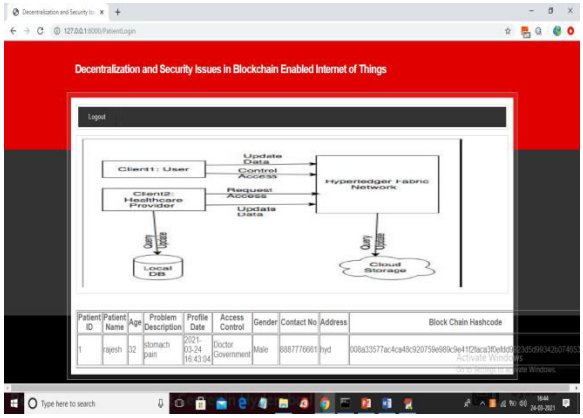


Fig.7: Patient login

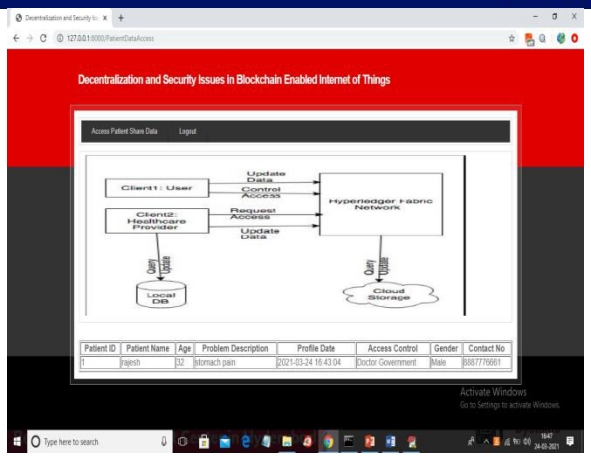


Fig.8: Access patient share data

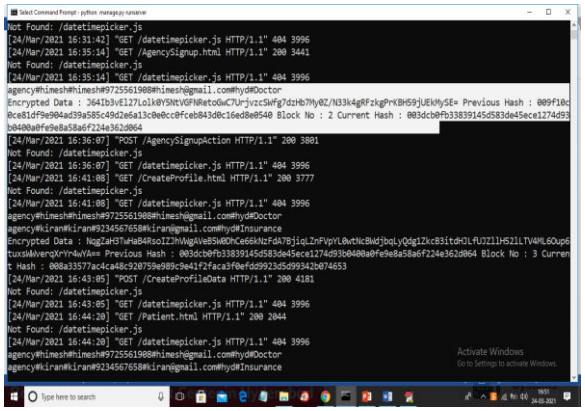


Fig.9: Hash code details

6. CONCLUSION

To accomplish the innovation's grand objectives of changing numerous parts of our general public and economy, IoT security and protection are pivotal achievement factors. Most of safety and security chances are tended to by our recommended blockchain-based IoT design, which additionally considers the asset impediments of numerous IoT gadgets. Our subjective above examination of the design uncovered that, best case scenario, it has steady above concerning execution, and to say the least, most of its exchanges scale with the quantity of groups as opposed to the quantity of hubs in the organization. Decentralized blockchain server that verifies previous hash codes at each transaction and stores data as blocks of trees; assuming check is effective, the information is thought of as unblemished; The Blockchain server notifies the

system that it is under attack and collects data from another functioning node if data changes. Blockchain is secure and reliable in today's market due to its immutable data storage and transaction hash code verification.

7. ACKNOWLEDGEMENT

We thank CMR Technical Campus for supporting this paper entitled "DECENTRALIZATION AND SECURITY ISSUES IN BLOCKCHAIN ENABLED INTERNET OF THINGS", which provided good facilities and support to accomplish our work. We sincerely thank our Chairman, Director, Deans, Head of the Department, Department of Computer Science and Engineering, Guide and Teaching and Non-Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work.

8. REFERENCES

1. Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. Comput. Netw. 2017, 112, 237–262.

2. Aldowah, H.; Rehman, S.U.; Umar, I. Security in Internet of Things: Issues, Challenges and Solutions. In International Conference of Reliable Information and Communication Technology; Springer: Cham, Switzerland, 2018; pp. 396–405.

3. Ourad, A.Z.; Belgacem, B.; Salah, K. Using blockchain for IOT access control and authentication management. In InternationalConference on Internet of Things 2018 June; Springer: Cham, Switzerland, 2018; pp. 150–164.

4. Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. J. Netw. Comput. Appl. 2019,144, 79–101.

5. Ouaddah, A.; Mousannif, H.; Ouahman, A.A. Access control models in loT: The road ahead. In Proceedings of the 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, Morocco, 17–20 November 2016;pp. 272–277.