International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 6, September-October 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

High Dimensional Health Care Privacy Approach Using Blockchain Technology with Emergency Medicine Tracking System Using Healthcare Supply Chain

Prof. Sunil Khatal[1], Miss. Divya Naikwadi[2], Prof. Monika Rokade[3]

[1]Assistant Professor, [2]PG Student, [3]Assistant Professor,
[1,2,3]Department 0f Comp Engineering, Sharadchandra Pawar College Of Engineering, Otur, Pune, Maharashtra, India

ABSTRACT

The blockchain typically described as a decentralized system in which transactional or ancient statistics are recorded, stored, and maintained throughout a peer-to-peer community of personal computers referred to as nodes. Counterfeit drugs are one consequence of such limitations within existing supply chains, which not only has serious adverse impact on human health but also causes severe economic loss to the healthcare industry. Blockchain technology has gained tremendous attention, with an escalating hobby in a plethora of several applications like safe and relaxed healthcare records management. Similarly, blockchain is reforming the traditional healthcare practices to an extra reliable means, in phrases of powerful prognosis and treatment through safe and cosy facts sharing using SHA Hash Generation Algorithm. Within the future, blockchain will be an era that can probably assist in personalized, authentic, and at ease healthcare by means of merging the entire actual-time scientific information of a patient's fitness and offering it in an up to date cosy healthcare setup. In this paper, we evaluation each the present and modern day trends inside the subject of healthcare with the aid of imposing blockchain as a model. We also talk the packages of blockchain, at the side of the demanding situations confronted and destiny views. The proposed system executed blockchain implementation in distributed computing surroundings and it gives the automated restoration of invalid chain by using Consensus and Mining Algorithm. In this system, we present a Custom blockchain-based approach leveraging smart contracts and decentralized off-chain storage for efficient product traceability in the healthcare supply chain. The smart contract guarantees data provenance, eliminates the need for intermediaries and provides a secure, immutable history of transactions to all stakeholders. We present the system architecture and detailed algorithms that govern the working principles of our proposed solution. We perform testing and validation, and present cost and security analysis of the system to evaluate its effectiveness to enhance traceability within pharmaceutical supply chains.

KEYWORDS: *Blockchain Technology, Decentralization / Decentralized System, Distributed Computing, Peer-to-Peer Network, Healthcare, Healthcare Supply Chain, etc*

How to cite this paper: Prof. Sunil Khatal | Miss. Divya Naikwadi | Prof. Monika Rokade "High Dimensional Health Care Privacy Approach Using Blockchain Technology with Emergency Medicine Tracking System Using Healthcare Supply Chain" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-6, October 2021, pp.1188-1193, URL: www.ijtsrd.com/papers/ijtsrd47555.pdf

IJTSRD47555

I. INTRODUCTION

A blockchain system considered as a virtually incorruptible cryptographic database where critical medical information could be recorded. A network of computers that is accessible to anyone running the software maintains the system. Blockchain operates as a pseudo-anonymous system that has still privacy issues since all transactions are exposed to the public, even though it is tamper-proof in the sense of data

integrity. The access control of heterogeneous patients' healthcare records across multiple health institutions and devices needed to be carefully designed. Blockchain itself is not designed as a large-scale storage system. In the context of healthcare, a decentralized storage solution would greatly complement the weakness of blockchain in the perspective.

The blockchain network as a decentralized system is more resilient in that there is no single-point attack or failure compare to centralized systems. However, since all the bitcoin transactions are public and everybody has access, there already exist analytics tools that identify the participants in the network based on the transaction history. With popularity analytics, similarity or closeness among topics within large volume of data can be detected. As information flows among different nodes in bitcoin network, Bitcoin transaction is slow because information needs to the propagated across the network to synchronize the ledger replicas. The slow dissemination of information exposes a potential security hole for the malicious attacks. However, long-term solutions are still required. Like any other networks, Bitcoin network is no exception when it comes to malicious attacks. One of the notable forms of attack against Bitcoin network topology is eclipsing attack by using information propagation knowledge. Bitcoin peer-to-peer network topology can inevitable and utilized by malicious attackers to perform precise attacks such as eclipsing attack. By observing the flooding process of the information flow, a flooding network's topology can inevitable. A network-topology inference approach has to propose along with a proof of concept in real network. The critical players of bitcoin transactions can be identified use various network centrality metrics. Blockchain might replace conventional methods of keeping track of valuable information such as contracts, intellectual-property rights, and corporate accountings. Personal healthcare records need to defend with the highest standard. With the increasing number of data breach incidents in the past several years, the awareness of the public about the personal data privacy will continue to increasing. The necessity for data privacy will grow stronger with an increasing number of services and device collecting our personal data associated with our personal identity.

II. LITERATURE SURVEY

- According to **Johansen, 2017** [2] Due to the novelty of concepts and the underlying technologies, the system provides a new overview on recent developments and related literature in this book and strives to explore the related concepts in the literature. Through the exploration of the concepts, the system dives into blockchain utilization as a technological platform for an upcoming ecosystem of applications and software and looks at the theoretical features of the technology as a foundation for this paper. Thus, systems enhance the understanding of the technology in other contexts throughout the literature and explore the current contributions to the literature. This study has implications for both researchers and practitioners. For researcher's systems seek to open research lines on enablement of the BT as a platform-centric technology for ecosystems to flourish as those of OI. For practitioners, systems illustrate that it is crucial to keep developing on the technology, as research indicates that systems have still not reached the tipping point of the technology.
- According to **Lember, 2017** [4]. The several technologies associated with the smart city, such as electronic sensors or urban control rooms and city labs. As well as emerging technologies, such as blockchain, that enables peer-to-peer service delivery is becoming more central to the ways citizens engage with public-service delivery under the schemes of dedicated user/citizen-innovation, technology, and living labs to accelerate technological innovations in the public sector. All these approaches aim at putting user experience at the center of the public sector innovation processes, however, these experimental units and methods are still far from becoming an organic part of the public sector and its change.
- According to **Pazaitis et al., 2017** [5] explores the potential of blockchain technology in enabling a new system of value that will better support the dynamics of social sharing. System study begins with a discussion of the evolution of value perceptions in the history of economic thought. Starting with a view on value as a mechanism that defines meaningful action within a certain context, the system associates the price system with the establishment of capitalism and the industrial economy. The system then discusses its relevance to the information economy, exhibited as the techno-economic context of the sharing economy, and identifies new modalities of value creation that had better reflect the social relations of sharing. Through the illustrative case of back end, new systems of value are anticipated, comprised of three layers: (a) production of value; (b) record of value; and (c) actualization of value. In this framework, the system discusses the solutions featured by Back feed and demonstrates a

conceptual economic model of blockchain-based decentralized cooperation.

- According to **Davidson et al. 2016** [1] as said, BT is a new institutional technology of governance that competes with other economic institutions of capitalism, namely firms, markets, networks, and even governments. Present this view of BT through a case study of Back feed, an Ethereum-based platform for creating new types of commons-based collaborative economies. This case was developed for evaluating contributions to projects on a network. Back feed introduces a social protocol on top of blockchain-based infrastructures to coordinate individuals through the creation and distribution of economic tokens and reputation scores. Its purpose after all allow for the emergence of meritocratic systems and emergent alternative economies that can variously augment or substitute for extant modes of economic governance (i.e. provided by hierarchies or markets). At its core, Backfeed is an engine for decentralized cooperation between distributed agents. It implements a Social Operating System for decentralized organizations, enabling massive open-source collaboration without any form of centralized coordination.
- According to **Glaser Bezzenberger, 2015** [3] following the theoretical introduction, this system aims to further elaborate on the theoretical grounding to give a summary of prior research and highlight potential areas for future research. Additionally, the system seeks to establish a common understanding of the theory within the field of OI regarding BT. Within the OI research area, BT has still considered a novel innovation and has yet to become a part of mainstream OI research. This is moreover supported by the general landscape, whose primary focus has been on the blockchain as a cryptographic economic system, e.g. Bitcoin.

III. PROPOSED WORK

The security challenges are still among the major obstacles when considering cloud adoption services. The main reason is that the database hosted and processed in the cloud server, which is beyond the control of the data owners. For the numerical query, these schemes do not provide sufficient privacy protection against practical challenges. In this system, we propose different data instance architectures for a secure database that protects several questions related to the numeric range. We implement a three-layer/instance storage framework based on data computing.

The technology of Blockchain attracts high attention first due to the possibility of decentralizing highly risky operations, which traditionally carried out in predetermined data centers. The most popular example of use is the replacement of the function of conducting transactions within the system of bank transfers to a decentralized network of cryptographic handlers. The essence of this method of processing financial transactions is the encryption of transaction sets combined into blocks with the inclusion in the code of the unique identifier code of the previous block.

- Large data storage at the required of decentralized data storage as well as an information system
- The different attack issues in centralized database architectures.
- There is no automatic attack recovery in central data architectures
- The decentralized architecture provides the automatic data recovery from different attacks.

After the analysis of this system, we move to develop the decentralized system architecture, and distributed computing provides parallel processing in a distributed environment.

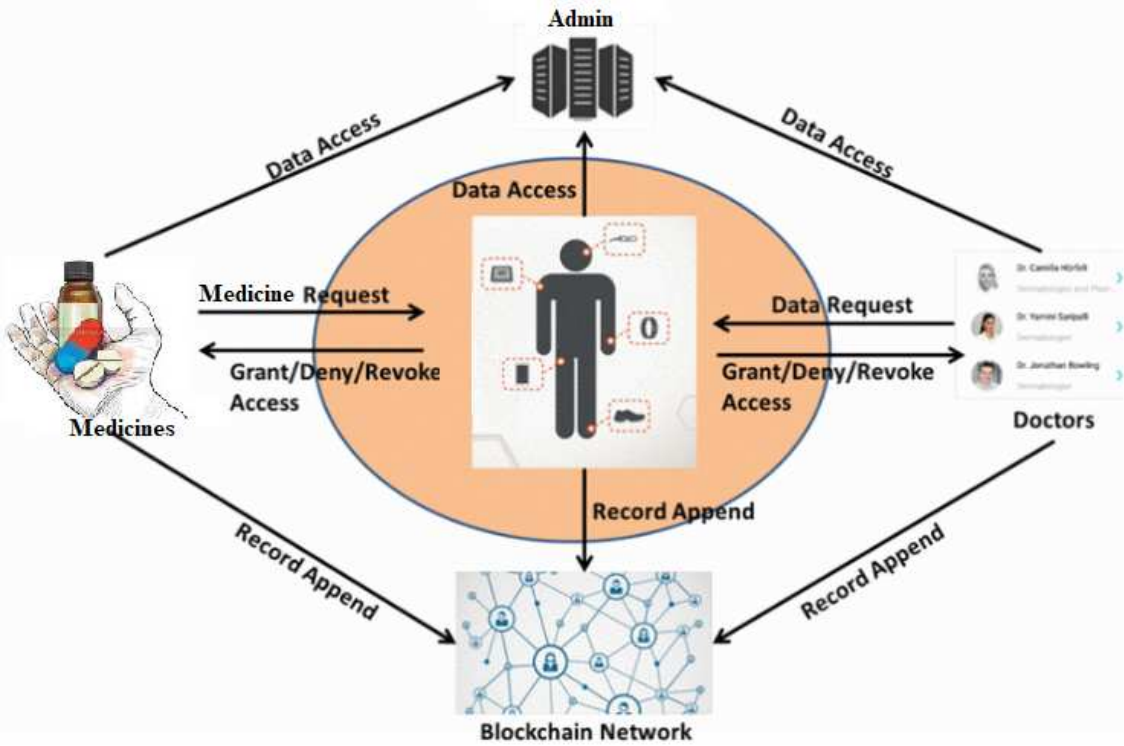

Fig.1: System Architecture

IV. OBJECTIVES

In this proposed model we are going to implement following things:

- To deisign appraoch for health insurance company where system store all hostorical data into block chain manner.
- To create a fog computing environment hierarcy for paralel data processing for end users applications.
- To design impelement own SHA family block for whole blockchain.
- Each transaction has stored on dependant blockchain in cloud environment.
- To design and implement a new mining technique for generate new block for each transaction.
- To imepement a varification algorithm which can validate each peer on every access request.
- To imepement emergency medicine tracking system and give to valid patients.

V. ALGORITHM

A. Blockchain:

Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure.

B. Custom Blockchain:

Custom Blockchain is a decentralized distributed database. The working processes of the system developed in this study are as follows:

Custom Blockchain provides low-cost off-chain storage to store supply chain transactions data to ensure reliability, accessibility, and integrity of the stored data. The integrity of data is maintained by generating a unique hash for every uploaded file on its server, the different hashes for the different uploaded files are then stored on the blockchain and accessed through the smart contract, and any change that occurs to any of the uploaded file is reflected in the associated hash.

C. Smart Contract:

Smart contracts are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met. At the most basic level, they are programs that run as they have been set up to run by the people who developed them for authentications. A smart contract is an agreement between two modules in the form of computer code. They run on the blockchain, so they are stored on a public database and cannot be changed. The transactions that happen in a smart contract processed by the blockchain, which means they can be sent automatically without a third party.

D. SHA Hash Generation:

The SHA-256 algorithm is a hashing algorithm that performs on data in one-way and Ron Rivist develops

it. It is an evolution of previous algorithms such as SHA 0, SHA 1, SHA 256, SHA 384. Hashing is also known as compression or message summary function, which takes the entire variable length and changes it into a binary sequence of fixed length.

VI. CONCLUSION

There are many research directions in applying Blockchain technology to the healthcare industry due to the complexity of this domain and the need for more robust and effective information technology systems. An interoperable architecture would undoubtedly play a significant role throughout many healthcare use cases that face similar data sharing and communication challenges. From the more technical aspect, much research is essential to pinpoint the most practical design process in creating an interoperable ecosystem using Blockchain technology while balancing critical security and confidentiality concerns in healthcare. Whether to create a decentralized application leveraging an existing Blockchain, additional research on secure and efficient software practice for applying the Blockchain technology in healthcare is also essential to educate software engineers and domain experts on the potential and limitations of this new technology. Likewise, validation and testing approach to gauge the efficacy of Blockchain-based health care architectures compared to existing systems are also important (e.g., via performance metrics related to time and cost of computations or assessment metrics related to its feasibility). In some cases, a new Blockchain network may be more suitable than the existing Blockchain; therefore, another direction may be investigating extensions of an existing Blockchain or creating a healthcare Blockchain that exclusively provides health-related services. Finally, we focus our contribution part that is the emergency medicine tracking system and give it to valid patients. This also determines the impact of those security issues and possible solutions, providing future security-relevant directions to those responsible for designing, developing, and maintaining distributed systems for patient data records and emergency medicines.

REFERENCES

[1] Gupta A, Patel J, Gupta M, Gupta H., (2017), Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1

[2] Navya A., Roopini R., SaiNiranjan A. S. et. Al, Electronic voting machine based on Blockchain technology and Aadhar verification, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)

[3] Hardwick, Freya Sheer, Raja Naeem Akram, and Konstantinos Markantonakis. "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy." arXiv preprint arXiv:1805.10258 (2018).

[4] Meter, Christian. "Design of Distributed Voting Systems." arXiv preprint arXiv:1702.02566 (2017).

[5] Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain."

[6] Martin A Makary and Michael Daniel. Medical error-the third leading cause of death in the us. BMJ: British Medical Journal (Online), 353, 2016

[7] Paul Tak Shing Liu. Medical record system using blockchain, big data and tokenization. In International Conference on Information and Communications Security, pages 254–261. Springer, 2016. [8] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on, pages 1–10. IEEE, 2013

[8] Till Neudecker, Philipp Andelfinger, and Hannes Hartenstein. Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences, pages 358–367. IEEE, 2016

[9] Dongsheng Zhang. Resilience enhancement of container-based cloud load balancing service. Technical report, PeerJ Preprints, 2018

[10] Dongsheng Zhang. Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks. PhD thesis, University of Kansas, 2015

[11] Dongsheng Zhang and James P.G. Sterbenz. Modelling critical node attacks in MANETs. In Self-Organizing Systems, volume 8221 of Lecture Notes in Computer Science, pages 127–138. Springer Berlin Heidelberg, 2014.

[12] Dongsheng Zhang and James P. G. Sterbenz. Analysis of Critical Node Attacks in Mobile Ad Hoc Networks. In Proceedings of the 6th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM),

pages 171–178, Barcelona, Spain, November 2014.

[13] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C¸ etinkaya, and James P.G. Sterbenz. Modelling Wireless Challenges. In Proceedings of the 18th ACM Annual International Conference on Mobile Computing and Networking (MobiCom), pages 423–425, Istanbul, August 2012. Extended Abstract.

[14] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C¸ etinkaya, and James P.G. Sterbenz. Modelling Attacks and Challenges to Wireless Networks. In Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pages 806–812, St. Petersburg, October 2012.

[15] Dongsheng Zhang and James P. G. Sterbenz. Measuring the Resilience of Mobile Ad Hoc Networks with Human Walk Patterns. In Proceedings of the 7th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), Munich, Germany, October 2015.

[16] Dongsheng Zhang and James PG Sterbenz. Robustness Analysis and Enhancement of MANETs using Human Mobility Traces. Journal of network and systems management, 24(3):653–680, 2016.

[17] Dongsheng Zhang and James P. G. Sterbenz. Robustness analysis of mobile ad hoc networks using human mobility traces. In Proceedings of the 11th International Conference on Design of Reliable Communication Networks (DRCN), Kansas City, USA, March 2015.