International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 02 | February - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Blockchain and Smart Contracts in a Decentralized Health Infrastructure

Dr.Vivek Waghmare, Gaurav Kolte, Gita Mutadak, Sanket Baviskar, Devashish Baviskar
Department of Information Technology
Sandip institute of Technology and Research centre Nashik, 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 progno- sis 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 trace- ability within pharmaceutical supply chains.

***Keywords*—** Blockchain Technology, Decentralization / Decentralized System, Distributed Com- puting, Peer-to-Peer Network, Healthcare, Supply chains, etc.

INTRODUCTION

A blockchain system can be considered as a virtually incorruptible cryptographic database where critical medical information and health supplychain could be recorded. The system is maintained by a network of computers, that is accessible to anyone running the software. Blockchain operates as a pseudo-anonymous system that has still privacy issue 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 the large-scale storage system. In the context healthcare, a decentralized storage solution would greatly complement the weakness of blockchain in the perspective.

Literature Survey

Map Reduce :-The author is Gupta A, Patel J, Gupta M, Gupta H. The advantages of this algorithm is the technology is more scalable, tamper proof and time stamped, making health data more secure. The limitation of this algorithm is Large amount of Dataset Required.

Map Reduce:- The author is Ariel Ekblaw, Asaph Azaria, John D. Halamka, Andrew Lippman. The advantages of this algorithm is this system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. The limitation of this algorithm is face a critical need for Electronic Health Records (EHRs).

Association Protocol :- The author is Jie Zhang Nian Xue and Xin Huang. The advantages of this algorithm is Propose a secure system for PSN-based healthcare. The limitation of this algorithm is Problem with a PSN node can securely share health data with other nodes in the network.

Advanced Encryption Standard :- The author is Saad Khan, Simon Parkinson and Yongrui Qin. The advantages of this algorithm is Fog systems are capable of processing large amounts of data locally, operate onpremise, are fully portable.

The limitation of this algorithm is Consuming limited amount of resources.

A Comprehensive Study of Visual Cryptography
Author: Jonathan Weir and WesiQi Yan, In this paper, we will summarize the latest developments of visual cryptography since its inception in 1994, introduce the main research topics in this area and outline the current problems and possible solutions. Directions and trends for future VC work shall also be examined along with possible VC applications.

A Novel Approach in Visual Cryptography
Author: Saptagiri,MRavikumar,DVenkanna, In this paper we represent we represents the novel technique to hide secret information pixel in to cover image with providing more visual quality of cover images compare to other technique.

An enhanced threshold visual secret sharing based on random grids. Author: Xuehu Yan, Xin Liu, Ching-Nung Yang, In this paper, a new threshold RG-based VSS scheme aiming at improving the visual quality of the previewed image is presented. Compared with previous schemes, our scheme can gain better visual quality in the reconstructed images as well as (k, n) threshold. In addition, the factor affecting the visual quality is analyzed and the differences between related approaches are discussed.

A novel template protection scheme for multi-biometrics based on fuzzy commitment and chaotic system. Author: Ning Wang, Qiong Li, Ahmed A. Abd El-Latif, JialiangPeng, Xuehu Yan, XiamuNiu, In this paper, a novel multi-biometrics template protection scheme based on fuzzy commitment and chaotic system, and the security analysis approach for unmoral biometrics leakage are proposed. Firstly, the thermal face images are captured to overcome the forgery.

Threshold construction from specific cases in visual cryptography without the pixel expansion.
Author: XuehuYan,ShenWang n, XiamuNiu, In this paper, three general threshold construction methods from specific cases are proposed. The constructed threshold VCSs are also progressive VCS without the pixel expansion. Analyses and experiments are conducted to evaluate the security and efficiency of the proposed methods.

Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions. Author: Song Wan, Yuliang Lu, Xuehu Yan, Yongjie Wang, Chao Chang1 Rece, In this paper, a novel visual secret sharing (VSS) scheme based on QR code (VSSQR) with (k,n) threshold is investigated. Our VSSQR exploits the error correction mechanism in the QR code structure, to generate the bits corresponding to shares (shadow images) by VSS from a secret biting the processing of encoding QR. Each output share is a valid QR code that can be scanned and decoded utilizing a QR code reader, which may reduce the selfhood of attracting the attentionof potential attackers. Due to different application scenarios, two different recovered ways ofthe secret image are given. The proposed VSS scheme based on QR code can visually reveal secret image with the abilities of stacking and XOR decryptions as well as scan every shadowimage, i.e., a QR code, by a QR code reader. The secret image could be revealed by human visualsystem without any computation based on stacking when no lightweight computation device. Onthe other hand, if the lightweight computation device is available, the secret image can be revealed with better visual quality based on XOR operation and could be lossless revealed when sufficient shares are collected. In addition, it can assist alignment for VSS recovery. The experiment results show the effectiveness of our scheme.

Problem Statement

In the proposed research work to design and implement a system for health care data and medicine tracking, where user can store all information in single blockchain without any Trusted Third Party (TTP) in fog computing environment. The system also carried out data integrity, confidentiality as well as eliminate the inconsistency for end user.

Objectives

• To design approach for distributed computing where system store all historical data into blockchain manner and work on chain consensus module.

• To create a distributed computing environment hierarchy for parallel data processing for end user's applications.

• To design implement own SHA family block for whole blockchain.

• Each transaction has stored on dependent blockchain in cloud environment.

• To design and implement a new mining technique for generate new block for each transaction.

• To implement a verification algorithm which can validate each peer on every access request.

• To provide drug traceability system using supply chain module.

Proposed System

Blockchain technology alleviates the reliance on a centralized authority to certify information integrity and ownership, as well as mediate transactions and exchange of digital assets, while enabling secure and pseudo-anonymous transactions along with agreements directly between interacting parties. Blockchain offers the opportunity to enable access to longitudinal, complete, and tamper-aware medical records that are stored in fragmented systems in a secure and pseudo-anonymous fashion.

The proposed work carried out blockchain implementation in distributed computing environment and it also provides the automatic recovery of invalid chain. 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.

Accordingly, existing studies have emphasized the need for a robust, end- to-end track and detect system for pharmaceutical supply chains. In that matter, an endtoend product tracking system across the pharmaceutical supply chain is main to ensuring product safety and removing counterfeits and drug trafficking issues.

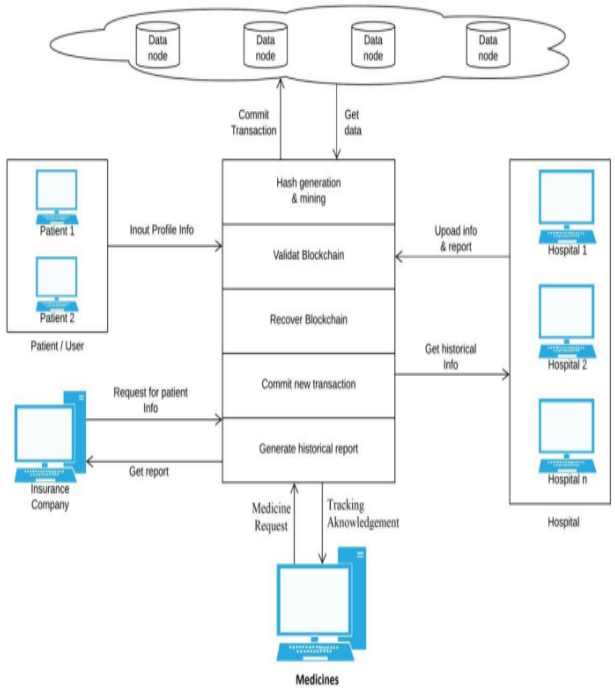

Fig. 1. Block Diagram

Hardware/Software Required Specifications

Software requirements-

- Operating system : Windows XP/7/LINUX.
- Front End : jsp (.html, .css, .js)
- Back End : MySQL 5.5 if required
- Tool/IDE : Eclipse Oxygen
- Server : Web Server (Tomcat 8.5)

Hardware requirements-

- System : Intel Core i3 2.40GHz.
- Hard Disk : 256 GB (Min)
- IO Devices : Mouse, Keyboard.
- Device Type : Laptop or Computer
- Ram : 4 GB (Min).

Outcomes

- We create a multiple land transnational data and stored all transnational data into multiple data nodes.
- Each node will hold the specific block for each transaction.
- Same block has replaced for all nodes, and generates a valid blockchain.
- System will retrieve data from all data nodes and commit the transaction, it should be any kind of DDL, DML as well as DCL transnational query.
- If any blockchain invalid during the validation of data servers, then system will automat- ically recover whole blockchain using majority of servers.
- We will address and eliminate the run-time server attacks and recover it using own blockchain.
- System will provide each transnational validation, for all servers.

Conclusion

In this paper, we have examined the challenge of medicine traceability inside pharmaceutical supply chains highlighting its significance especially to protect against counterfeit medicine and medicine trafficking. We have developed and determined a blockchain-based solution for the pharmaceutical supply chain to track and trace medicine in a decentralized manner. Specif-ically, our proposed solution holds cryptographic fundamentals of block-chain technology to achieve protected logs of events

within the supply chain and uses smart contracts within Cus-tom blockchain to achieve automated recording of events that are accessible to all participating collaborators.

We will continue our efforts to increase the efficiency of pharmaceutical supply chains and imagine focusing on extending the proposed system to achieve end-to-end transparency and provability of medicine use as future work.

Future Scope

- In the future, we will further improve the blockchain powered parallel healthcare systems (PHS) and make it available for more disease treatments scenarios.
- In future scope we also include the disease prediction model in our proposed work.

References

[1] L. Guo, C. Zhang, J. Sun, Y. Fang. "A privacy-preserving attribute based authentication System for Mobile Health Networks," IEEE Transactions on Mobile Computing, 2014, vol. 13, no. 9, pp. 1927- 1941.

[2] A. Abbas, S. Khan, "A review on the state-of-the-art privacy preserving approaches in e-health clouds," IEEE Journal of Biomedical Health Informatics, 2014, vol. 18, pp. 1431-1441.

[3] J. Yang, J. Li, Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, 2015, vol. 43-44, pp. 74-86.

[4] http://www.pbs.org/newshour/updates/has-health-care-hacking -become-an-epidemic/.

[5] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13thm ACM Conf. Computer and Comm. Security (CCS'06), pp. 89-98, 2006.

[6] R. Ostrovsky, A. Sahai, B.Waters, "Attribute-based encryption with nonmonotonic access structures," in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195-203.

[7] J. Han, W. Susilo, Y. Mu. "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," IEEE Transactions on on Information Forensics and Security, 2015, vol. 10, no. 3, 665-678

[8] M. Li, S. Yu, Y. Zheng, K. Ren,W. Lou. "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE transactions on parallel and distributed systems, 2013, 24(1): 131-143.

[9] M. Green, S. Hohenberger, B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

[10] J. Lai, R. H. Deng, C. Guan, J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.

[11] B. Qin, R. H. Deng, S. Liu, S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1384-1394, JULY. 2015

[12] Spvryan's International Journal of Engineering Sciences & Technology (SEST) ISSN : 2394-0905 "Design of a Cloud Based Emergency Healthcare Service Model"