International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 04 | April - 2021 ISSN: 2582-3930

DECENRALIZED MEDICAL DATA SHARING USING CLOUD COMPUTING

Dhatchayani D[1], Vinitha S[2],Sivaranjini R[3]
[12]Student, [3]Assistant Professor, Department of CSE

Krishnasamy College of Engineering & Technology ,Cuddalore

***Abstract*--In this project, the block chain is fully decentralized. In addition, digital signatures are required for model updates. Therefore, we hold that adversaries are not able to fabricate digital signatures or take control of the majority of the network. Furthermore, an adversary cannot poison the data because it is stored off-chain rather on the public ledger. There are only pointers information encrypted with a hash function inside a public ledger. In view of the problems of large-grid-level centralized transactions and dispatch centers with information asymmetry and high processing costs, a completely decentralized transaction architecture and a weak centralized scheduling strategy based on block-chain are proposed. Firstly, the concepts of transaction decentralization and scheduling decentralization are defined, and the reliability of distributed transaction communication is studied. Built a block chain transaction risk control model based on the communication credit consensus mechanism. Secondly, under the weakly centralized scheduling architecture based on the autonomous chain of substations, security checks are performed, and temporary central nodes are set up to perform scheduling tasks. Finally, an improved evolutionary game algorithm is used to solve the above model, and the optimal solution is obtained by dynamically updating the credibility.**

I. INTRODUCTION

A block chain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data .

Block chain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the crypto currency bit coin.

The invention of the block chain for bit coin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bit coin design has inspired other applications, and block chain that are readable by the public are widely used by crypto-currencies. Block chain is considered a type of payment rail.

Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the block chain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any block chain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others.

Block Time

The block time is the average time it takes for the network to generate one extra block in the block chain. Some block chains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In crypto currency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bit coin it is 10 minutes.

Decentralization

By storing data across its peer-to-peer network, the block chain eliminates a number of risks that come with data being held centrally. The decentralized block chain may use ad-hoc message passing and distributed networking.

Peer-to-peer block chain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Block chain security methods include the use of public-key cryptography. A public key (a long, random-looking string of numbers) is an address on the block chain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that block chains now support. Data stored on the block chain is generally considered incorruptible.

II. OBJECTIVE

The main objectives of this project is the block chain, which is tamper-proof and requires a large enough network to avoid un trusted end devices taking over it which is that end devices can properly secure their keys during the operations.

III. LITERATURE REVIEW

A. ACAR, H. AKSU, A. S. ULUAGAC, AND M. CONTI, ``A SURVEY ON HOMOMORPHICENCRYPTION SCHEMES: THEORY AND IMPLEMENTATION," ACM COMPUT. SURV., VOL. 51, NO. 4, JUL. 2018, ART. NO. 79.

Intellectual property (IP) core of digital signal processing (DSP) kernels act as hardware accelerators in consumer electronics (CE) systems. However due to rising threats of cloning and counterfeiting to an IP core, security remains an important subject of research for these hardware accelerators. This paper presents a novel key-driven hash-chaining based hardware steganography for securing such IP cores used in CE systems. The proposed approach is capable to implant secret invisible stego-marks in design using hash-chaining process that incorporates switches, strong large stego-keys, multiple encoding algorithms and hash blocks. The methodology proposed provides massive security against IP cloning and counterfeiting while incurring nominal design overhead (<0.3 %). The results of the proposed approach on comparison with state of the art indicated significantly stronger digital evidence (lower probability of co-incidence), stronger key size (in bits) and lower design cost using proposed stego-marks. Further, from an attacker's perspective, the proposed steganography increases an attacker's effort manifold during decoding the valid stego-key value (for generating/extracting original secret stego-mark), compared to existing approaches.

B. PRYBILA, S. SCHULTE, C. HOCHREINER, AND I.WEBER, ``RUNTIME VERIFICATION FOR BUSINESS PROCESSES UTILIZING THE IOMT BLOCKCHAIN," FUTURE GENER. COMPUT. SYST., VOL. 107, PP. 816831, JUN. 2020.

The most burning topic of today, calls for a holistic solution that is reliable, secure, privacy preserved, cost effective Cloud storage that can tide over the turbulent conditions of the rapidly budding digital storage technologies. This send an outcry for a devoted solution, in the form of an individualized, patient-centric care - IoMT that augments precise disease identifications, decrease in errors, reduction in costs of care through the support of technology, allows patients to direct health information data to doctors, manage drugs, keep Personal Health Records, caters to remote medical supports Care, provides proactive approach to preserving Good Health, improves and

Accelerates Clinician Workflows, empowers extreme connectivity due to better automation and perceptions in the DNA of IoMT functions. But IoMT adoption is like a rose with thorns like constraints of increased administrative costs, deficiency of universal data access, present-day electronic medical records. The BCT is used in the framework to overcome the security issues of IoMT through the use of latest encryptions. Furthermore, this framework harnesses the benefits of Block Chain like reduced cost, speed, automation, immutability, near-impossible loss of data, permanence, removal of intermediaries, decentralization of consensus, legitimate access to health data, data safekeeping, accrual-based imbursement mechanisms, and medical supply chain efficacy. The outcomes in this paper are (i)A systematic investigation of the current IoMT, Block Chain and Cloud Storage in HealthCare;(ii) Explore the challenges and necessities for the confluence of Block Chain (BC), Internet of Medical Things (IoMT), Cloud Computing (CC);(iii)Formulate the requirements necessary for the real-time remote Health Care of one-to-one care structure, which, supports the vital functions that are critical to the Patient Centric Health Care;(iv) Design and develop a novel BC IoMT U6 HCS (Block Chain based Internet of Medical Things for Uninterrupted, Ubiquitous, User-friendly, Unblemished, Unlimited Health Care Services) Layered Architecture, to support the vital functions critical for Patient Centric Health Care and (v) Implement and test with the previous established and proven techniques.

IV. SYSTEM ARCHITECTURE

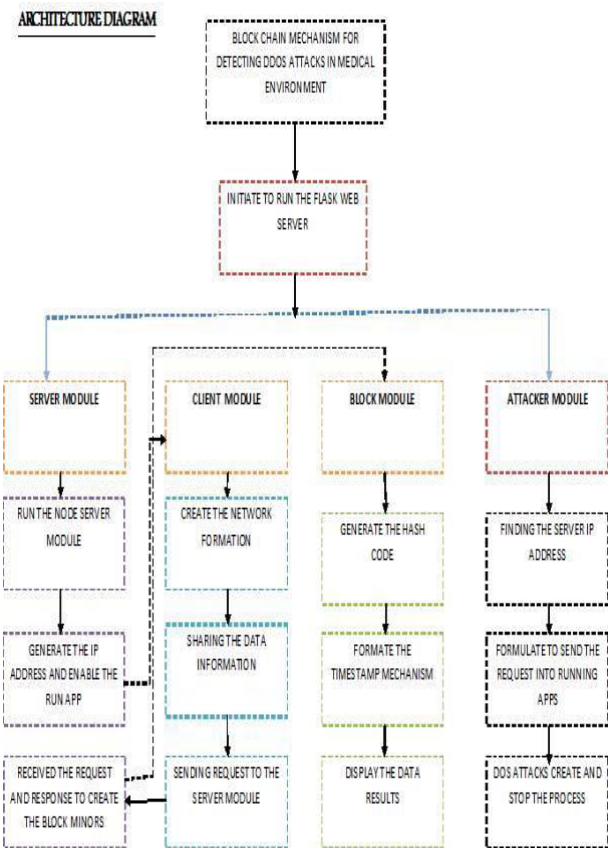


Figure: Architecture Diagram

V. MODULE DESCRIPTION

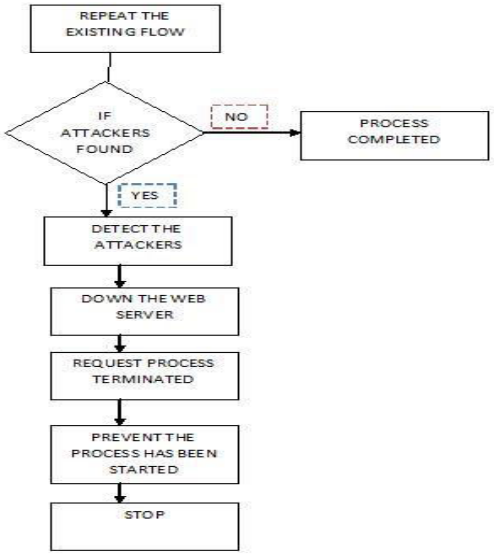
Decentralization module

By storing data across its peer-to-peer network, the block chain eliminates a number of risks that come with data being

held centrally. The decentralized block chain may use ad hoc message passing and distributed networking.

Node Server Module

Block chain is decentralized, encrypted, and cross-checked which allows the data to remain strongly backed. As block chain is fully loaded with nodes and to hack most of the nodes concurrently it is impossible. Being one of distributed ledger technology it's most fundamental attributes are data immutable.



App Module

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the block chain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Block Chain Training Module

Block chain systems use asymmetric cryptography to secure transactions between users. In these systems, each user has a public and private key. It is mathematically impossible for a user to guess another user's private key from their public key. This provides an increase in security and protects users from hackers.

Attackers Module

A Denial-of-service attack (DoS attack) is an attempt to make a computer or network resource unavailable to its intended users. This causes a Denial of Service (DoS) and results in slow access to the Internet, since the amount of traffic attempting to ping your IP address overloads the router.

IV. CONCLUSION

We propose a novel block chain enabled federated learning model to solve the identified issues in flask web server in python. End devices upload the local updates to the node servers, where the global updates will be generated and stored. Since only the pointer of the global updates is saved on-chain while a distributed hash table (DHT) is used to save to data, the block generation efficiency could be guaranteed. With a hybrid identity generation, comprehensive verification, access control, and off-chain data storage and retrieve, Block enables decentralized privacy protection while preventing single point failure. Extensive evaluation results on real-world datasets are presented to show the superiority of Block. For future work, we plan to further extend this model to more generalized scenarios by optimizing the trade-off between privacy protection and efficiency. In addition, we prepare to use game theory and Markov decision process to identify the optimal conditions in terms of computation and communication costs.

REFERENCES

[1] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, ``A survey on homomorphic encryption schemes: Theory and implementation," ACM Comput. Surv., vol. 51, no. 4, Jul. 2018, Art. no. 79.

[2] S. Angraal, H. M. Krumholz, andW. L. Schulz, ``Block chain technology: Applications in health care," Circulat., Cardiovascular Qual. Outcomes, vol. 10, no. 9, 2017, Art. no. e003800.

[3] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ``MedRec: Using block chain for medical data access and permission management," in Proc. IEEE OBD, Vienna, Austria, Aug. 2016, pp. 2530.

[4] O. Attia, I. Khou, A. Laouiti, and C. Adjih, ``An IoT-blockchain architecture based on hyperledger
framework for healthcare monitoring application," in Proc. 10th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS), Jun. 2019, pp. 15.

[5] A. Baliga. (2016). The Block
Chain Landscape. Persistent Systems. Accessed: Oct. 20, 2020.
[Online]. Available: https://columbus.org/wpcontent/ uploads/2018/10/wp_the-blockchain-landscape.pdf

[6] G. Baxendale, ``Can blockchain revolutionise EPRs?" ITNOW, vol. 58, no. 1, pp. 3839, Mar. 2016.

[7] M. Benchou and P. Ravaud, ``Block chain technology for
improving clinical research quality," Trials, vol. 18, no. 1, p. 335, 2017.

[8] B. Xu, L. Xu, H. Cai, L. Jiang, Y. Luo, and Y. Gu, ``The design of an m-Health monitoring system based on a cloud computing platform," Enterprise Inf. Syst., vol. 11, no. 1, pp. 1736, 2015.