Journal of Ubiquitous Computing and Communication Technologies (ISSN: 2582-337X)
www.irojournals.com/jucct/

Metadata Securing Approach on Ubiquitous Computing Devices with an Optimized Blockchain Model

S. Ayyasamy

Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

E-mail: ayyasamyphd@gmail.com

Abstract

Metadata is an exploration of the given data. It organizes the data by grouping the collected information on a particular structure for easy understanding. Metadata reduces the computational burden on data mining algorithms by keeping an organized record. Data that are related to healthcare application requires serious attention on privacy concern and therefore such information are encrypted in most cases. Processing of encrypted data is difficult, and it may lead to estimate the prediction with a faulty output. Hence, a blockchain based data securing system is proposed in the work for securing the data that are transmitted from a ubiquitous computing device. The paper also incorporates the proposed work with a whale optimization algorithm for reducing the execution time required on the blockchain based data storage and retrieval process.

Keywords: Pervasive computing, metadata privacy, wearable devices, smart healthcare measurement, blockchain iteration, whale optimization

1. Introduction

Ubiquitous computing devices are also called as pervasive computing devices that allow the smart electronic device to operate certain simple computations with the help of microprocessor inbuilt with it. In most cases, the ubiquitous devices are connected with cloud storage through an internet connection for storing the collected data. The ubiquitous devices also work same as that of IoT device but it has an inbuilt data storage and processing unit. The technologies behind a ubiquitous device is shown in figure 1. The electronic technologies involved in the ubiquitous devices need to be small in size with less energy consumption

DOI: https://doi.org/10.36548/jucct.2022.2.001
Received: 11.05.2022, received in revised form: 09.06.2022, accepted: 24.06.2022, published: 04.07.2022

components. Sensors are one of the primary interfacing components in such devices for gathering information [1, 2].

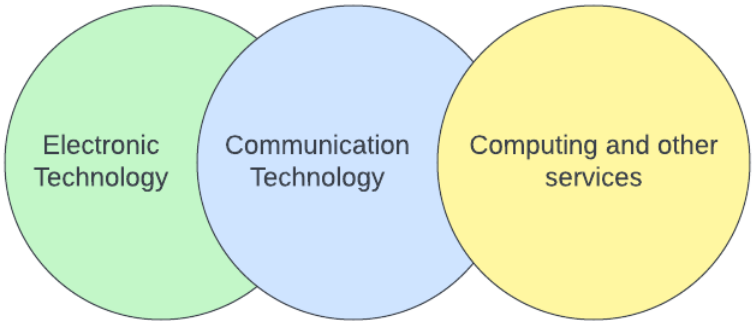

Figure 1. Concepts behind the ubiquitous technology

The IoT based communication systems are interfaced with the ubiquitous devices that consist of larger bandwidth and higher data transfer rate for improving their efficiency. Similarly, a computing module is integrated with the ubiquitous device for processing the collected data [3]. The basic characteristics of ubiquitous computing system are as follows.

- Integration of multiple systems into a single device.
- Optimized interfacing module for giving a better user experience.
- Simultaneous process on online and offline data.
- Connected to cloud and specialized local systems for data operation.
- Secured data communication with authorized access.
- Operational customization.

1.1 Benefits, Challenges and Applications of Ubiquitous Computing

The ubiquitous computing devices are highly beneficial to their nature on integration with multiple sensor and small size occupancy. Its nature on scheduling improves the user experience to certain extent and that also allows the device to schedule its data sharing process with good efficiency. As the energy consumption of ubiquitous devices are very low, it can be placed in a remote location too for gathering information with a small solar panel or battery support [4, 5]. Privacy is one of the primary challenges in the ubiquitous devices and that requires an algorithmic operation for protecting the data. At the same time, the hardware

and software security also make a limitation on implementing the device to many applications like healthcare and environmental monitoring [6]. However, the ubiquitous are devices are successfully implemented in the areas mentioned in figure 2.

Figure 2. Applications of ubiquitous computing

2. Literature Survey

A blockchain based decentralized system was designed to secure the information gathered on ubiquitous learning environment. The data were transmitted in the work through a miner module that observes the transaction on each communication [7]. Blockchain and Distributed Ledger-based Improved Biomedical Security system was proposed to enhance the privacy on the healthcare data. The experimental work also indicated a remarkable performance on its access speed on multiple transactions [8]. An SHA256 hash algorithm was structured to specify the location of each block involved in the blockchain environment. Hence it did not allow the data stored in the block to move from one place to another place. The analytic model gives betterment in terms of authentication count and delay [9].

A blockchain based security model was developed for cloud-based encryption system to protect the data sharing medium between the user application to the consumer application layer. The concept allowed to share data on very huge quantity in an encrypted format [10]. Hyperledger based electronic healthcare record system was structured with the concept of chain code for securing the healthcare data. The performance of the proposed model produced a better outcome at throughput measurement and round-trip time assessment [11].

A blockchain based approach called healthchain was framed to secure the large scale healthcare data on sharing information between the patient and doctor. The motive of the

work was to secure the information from manipulation and deletion without the user knowledge. The experiment showed an improvement on communication and computation costs [12]. A decentralized data storage system was designed with interplanetary file system for storing the secured information of patient health records. A hyperledger caliper tool was incorporated in the work to calculate the throughput and latency of the proposed concept in a blockchain environment [13].

An electronic healthcare storage system based on blockchain approach was implemented to a centralized cloud system for data securing purpose. The work utilized searchable encryption protocol along with a re-encryption proxy network for realizing the security. The performance evaluation satisfied the computational efficiency on its higher side [14]. The blockchain technology was also included to the telehealth and telemedicine system for providing a data traceability and immutability on data theft. The blockchain methodologies were safe due to their nature on decentralization and transparency [15]. A cryptographic technique was merged over the traditional blockchain method for preserving the electronic healthcare records over the cloud system. The work allowed the data transaction based on the requests received from the transaction creation on the user [16].

A novel decentralized authentication algorithm was structured to organize the patient data on a blockchain network. The performance of the proposed model was compared with the traditional cloud system model without a blockchain environment. It indicated a good outcome on the authentication delay and network utilization [17]. A blockchain-assisted secure data management framework was organized to manage the healthcare data in a secure manner. The technique was analyzed the data transaction made between the implantable medical devices to the hospital private servers. The experimental model showed betterment on response time and accuracy ratio at a remarkable rate [18].

A keyless signature infrastructure was designed to access the blockchain network for storing the healthcare data. An experiment was performed to analyze the outcome on average time, size, and cost on data access. The performance analysis gave a satisfaction on accessing speed and data storage occupancy [19]. An attribute based encryption model was proposed for securing the healthcare data to be stored on the cloud system. The system creates a new block when there is a transaction presence in the blockchain system. The experimental model showed a reduction in average time of operation data and execution time, and it improved the success rate over the traditional models with a great deviation [20].

3. Proposed Method

Blockchain is a system used for securing the information in a distributed manner at a digital ledger environment. The blockchain modules does not require any third party algorithm or application for saving the stored information and it's the main advantage of using blockchain in many applications. It is achieved by storing the data on different block by segregating the collected information into a group. The storage capacity of the block defines the amount of data that can be stored. The storage completed blocks are structured to make a chain connection over their previous blocks for data continuity. A new block will be opened in the chain process for storing the new upcoming data. In some applications, multiple blocks are opened for storing the categorized information. Figure 3 represents the transactional process view of a blockchain system.

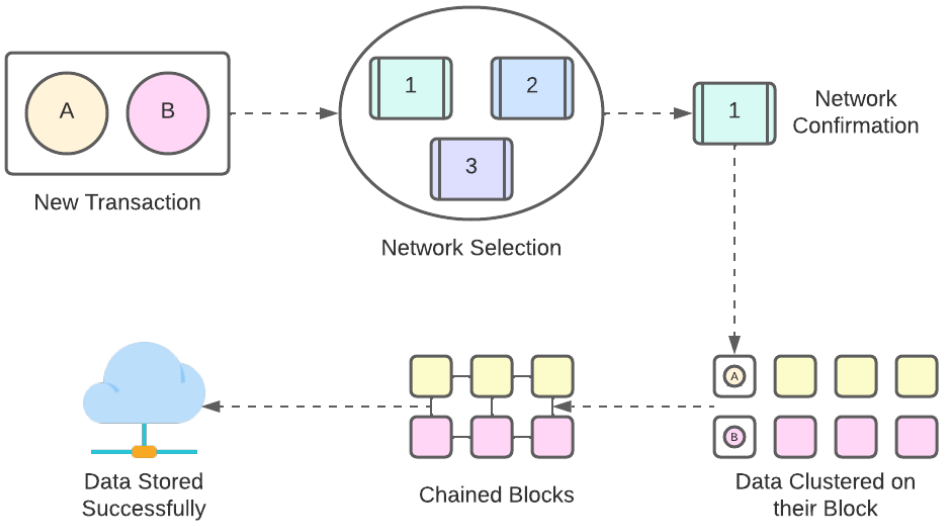

Figure 3. Blockchain transaction process

A new transaction consisting of two different data 'A' & 'B' is shown in the process transaction figure and they are further forwarded from the base station to the cloud network for selecting their appropriate cloud system for storing the data. After selecting the network with confirmation, the data are stored in their respective distributed blocks. The completed blocks are grouped to form a chain architecture for final data storing process. Due to the complexity of the blockchain transaction process, the time required for data storing and retrieval becomes little high in some cases. To enhance such timing issue, certain optimization algorithms were utilized so far. In the proposed work, a whale optimization

approach is employed and its performances are verified over a blockchain model without optimization module.

3.1 Whale Optimization Algorithm (WOA)

WOA is a kind of meta-heuristic approach widely implemented to solve the numerical problems. The algorithm was developed from the inspiration of bubble net and social activity of whales in the ocean. Bubble net is a process of foraging done by whales by creating bubbles in a circular manner. The process of bubble net can be mentioned in two ways as upward spirals and double loops. In WOA, the bubble net model is implemented mathematically for searching a best solution by creating an encircling prey. The current best solution is moved towards the target solution in a step by step manner. The remaining solutions also change their position to reach the targeted solution as shown in equation 1.

$$X\ (t+1) = Xbest\ (t) - A.D \tag{1}$$

where, t = present iteration

A&D = attribute coefficients

Xbest = best position vector

In shrink enriching process the value of the vectors are changed randomly to reach the level of zero. The updated position is represented in equation 2.

$$X\ (t+1) = Xbest\ (t) + D.e.cos2\pi \mathrm{L} \tag{2}$$

where, L = random location from -1 to 1

4. Experimental Work

The performance of the proposed work is experimented in Python environment and a group of random transaction is generated in the work to estimate the efficiency of the blockchain model with and without WOA optimization method. Figure 4 represents the memory utilization of the experimented work with respect to the number of blocks considered for the transaction. It indicates a gradual deviation on memory utilization with and without optimization model. Hence, the optimization model provides a better utilization of the resource for long term running process.

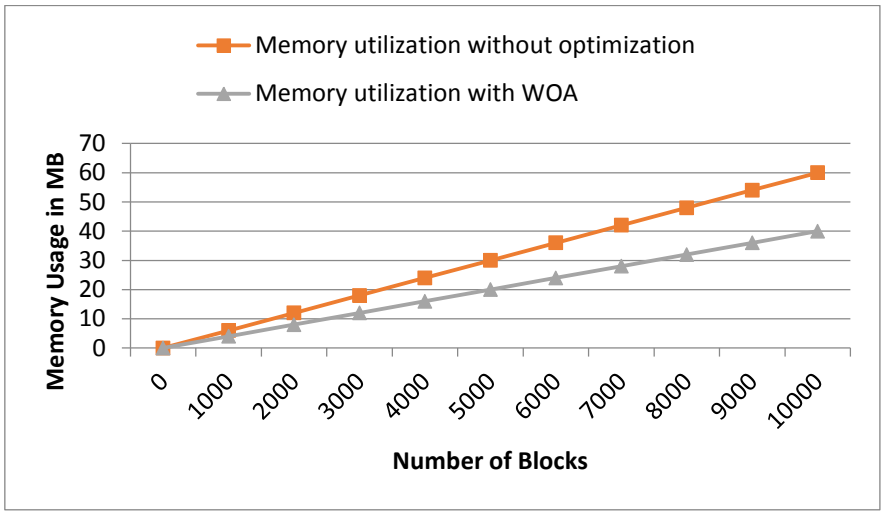

Figure 4. Memory utilization vs number of blocks

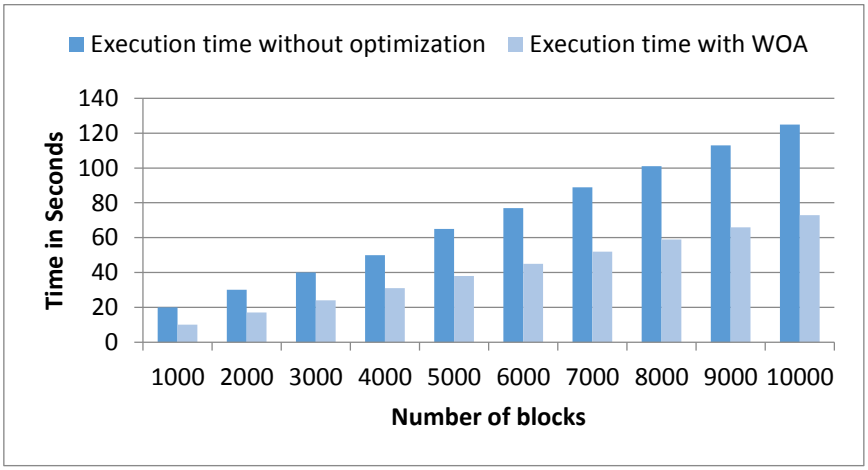

Figure 5. Execution time on chain verification process

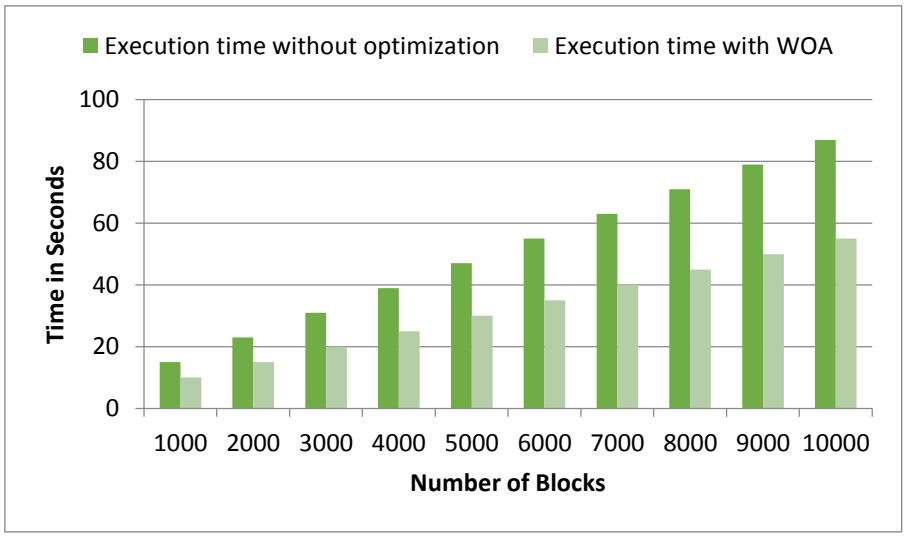

Figure 6. Execution time on chain retrieval process

The performance of the proposed work is compared to that of the traditional technique in terms of the execution speed at the time of data verification process on storing it to the appropriate blockchain and its outcome is projected in figure 5. The execution time of the model without optimization is not gradual, and a slight surge at the incremental side is observed after 5000 blocks; but in case of optimized model such surges are not observed at any block interval.

The execution time on the retrieval process is always less when comparing to the storage time on any system and that is clearly reflected in the conducted experiment projection shown in figure 6. The retrieval time on the optimized model shows betterment but the deviations are gradual in the retrieval process, whereas in chain verification process it is not gradual for non-optimized model.

5. Conclusion

In recent days, the ubiquitous devices are employed in many applications due to the development on reliability in internet connectivity with good data transfer rate. The data that are created from such devices are stored in the cloud environment as metadata for improving the data access convenience. A WOA based optimization algorithm is employed in the proposed work for securing the cloud metadata in an efficient manner with blockchain technology. An experimental study is conducted with Python environment by generating a random data transaction to the blockchain network. A comparative analysis is performed over the traditional blockchain model without any optimization technique and found satisfied with the proposed WOA based optimization model in terms of execution time and memory utilization rate. In future, the experiment will be further conducted with different optimization algorithms to find a better optimization model.

References

[1] Mukhametov, D. R. "Ubiquitous computing and distributed machine learning in smart cities." In 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), pp. 1-5. IEEE, 2020.

[2] Bardram, Jakob E., and Aleksandar Matic. "A decade of ubiquitous computing research in mental health." IEEE Pervasive Computing 19, no. 1 (2020): 62-72.

[3] Cui, Yuanhao, Fan Liu, Xiaojun Jing, and Junsheng Mu. "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges." IEEE Network 35, no. 5 (2021): 158-167.

[4] Bardram, Jakob, and Adrian Friday. " Ubiquitous Computing Systems." In Ubiquitous Computing Fundamentals, pp. 51-108. Chapman and Hall/CRC, 2018.

[5] Dhyani, Kshitij, Saransh Bhachawat, J. Prabhu, and M. Sandeep Kumar. "A Novel Survey on Ubiquitous Computing." In Data Intelligence and Cognitive Informatics, pp. 109-123. Springer, Singapore, 2022.

[6] Mao, Shitong, Yassin Khalifa, Zhenwei Zhang, Kechen Shu, Anisha Suri, Zeineb Bouzid, and Ervin Sejdic. "Ubiquitous computing." In Digital Health, pp. 211-230. Academic Press, 2021.

[7] Bdiwi, Rawia, Cyril De Runz, Sami Faiz, and Arab Ali Cherif. "A blockchain based decentralized platform for ubiquitous learning environment." In 2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT), pp. 90-92. IEEE, 2018.

[8] Liu, Haibing, Rubén González Crespo, and Oscar Sanjuán Martínez. "Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts." In Healthcare, vol. 8, no. 3, p. 243. MDPI, 2020.

[9] Rajawat, Anand Singh, Romil Rawat, Kanishk Barhanpurkar, Rabindra Nath Shaw, and Ankush Ghosh. "Blockchain-based model for expanding IoT device data security." In Advances in Applications of Data-Driven Computing, pp. 61-71. Springer, Singapore, 2021.

[10] Zheng, Xiaochen, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. "Blockchain-based personal health data sharing system using cloud storage." In 2018 IEEE 20th international conference on e-health networking, applications and services (Healthcom), pp. 1-6. IEEE, 2018.

[11] Tanwar, Sudeep, Karan Parekh, and Richard Evans. "Blockchain-based electronic healthcare record system for healthcare 4.0 applications." Journal of Information Security and Applications 50 (2020): 102407.

[12] Xu, Jie, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, and Nenghai Yu. "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data." IEEE Internet of Things Journal 6, no. 5 (2019): 8770-8781.

[13] Zaabar, Bessem, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Mohamed Abid. "HealthBlock: A secure blockchain-based healthcare data management system." Computer Networks 200 (2021): 108500.

[14] Wang, Yong, Aiqing Zhang, Peiyun Zhang, and Huaqun Wang. "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain." Ieee Access 7 (2019): 136704-136719.

[15] Ahmad, Raja Wasim, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Samer Ellahham, and Mohammed Omar. "The role of blockchain technology in telehealth and telemedicine." International journal of medical informatics 148 (2021): 104399.

[16] Sharma, Yogesh, and B. Balamurugan. "Preserving the privacy of electronic health records using blockchain." Procedia Computer Science 173 (2020): 171-180.

[17] Yazdinejad, Abbas, Gautam Srivastava, Reza M. Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Mohammed Aledhari. "Decentralized authentication of distributed patients in hospital networks using blockchain." IEEE journal of biomedical and health informatics 24, no. 8 (2020): 2146-2156.

[18] Abbas, Asad, Roobaea Alroobaea, Moez Krichen, Saeed Rubaiee, S. Vimal, and Fahad M. Almansour. "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things." Personal and Ubiquitous Computing (2021): 1-14.

[19] Nagasubramanian, Gayathri, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya, and Balamurugan Balusamy. "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud." Neural Computing and Applications 32, no. 3 (2020): 639-647.

[20] Mubarakali, Azath. "Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach." Mobile Networks and Applications 25, no. 4 (2020): 1330-1337.

Author's biography

S. Ayyasamy obtained his Bachelor's degree in Electronics and Communication Engineering from "Maharaja Engineering College, Avinashi" under Bharathiyar University and Masters Degree in Computer Science and Engineering from "PSG College of Technology, Peelamedu, Coimbatore." under Bharathiyar University. He completed his Ph. D in the area of Peer to Peer Overlay Networks under Anna University, Chennai. He has more than 19

years of teaching experience. He is currently working as Professor in the School of Computer Science and Engineering at Vellore Institute of Technology, Vellore, India. He has been working as Reviewer for reputed journals like Human-computer Interaction journal -Taylor & Francis, Journal of Network and Computer Applications–Elsevier and Information Security Journal-Inderscience. He was also working as the Editor for International journal of Engineering Technology and Science. He was acted as coordinator for the Establishment of New Course B. Arch and Information Technology lab, for conducting Info science microsoft conference RACHNA'09, for the Recognition of Anna University Research Center, to start a new journal entitled "International Innovation Journal of Engineering and Applied Research" through SRDC, Infosys Campus Connect Assistant Coordinator and many more prestigious activities. His Research areas of interest are Peer to Peer Networks, Overlay Networks, Automation, Machine learning and Artificial Intelligence.