Secure Authentication in IoT Based Healthcare Management Environment Using Integrated Fog Computing Enabled Blockchain System

Parag Verma, Rajeev Tiwari, and Wei-Chiang Hong

1 Background

Internet of Things (IoT) has emerged very rapidly in the field of technology in the recent few years. There has been a rapid change in the industry of medical devices and services provided by them. With the help of the Internet of Medical Technology, very important advantages are being received in the field of medical services, in which diagnostic tools are connected with each other and with the help of which one can get health-related information anytime and anywhere. The development and rise of Internet of Things in the medical field can play an important role in improving the quality of life of citizens by enabling Internet of Medical Technology based health monitoring systems that can control the limitations of time and location. Also, this technology can be used to provide individual and user-focused healthcare services. Because Internet of Things based health monitoring systems in medical work by integrating various medical devices such as biosensors, actuators, wireless access points etc. with various communication technologies such as WLAN, Bluetooth, Zigbee etc. to synchronize and exchange data. Internet access at this point raises many challenges to the security and privacy of personal and confidential health care information. In this way, security systems that meet key security requirements (i.e.,

P. Verma
Chitkara University, Rajpura, Punjab, India

R. Tiwari (✉)
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India

W.-C. Hong
Asia Eastern University of Science and Technology, New Taipei, Taiwan

Yuan Ze University, Chungli, Taiwan

R. Tiwari et al. (eds.), *Image Based Computing for Food and Health Analytics: Requirements, Challenges, Solutions and Practices*,
https://doi.org/10.1007/978-3-031-22959-6_8

user authentication, user authorization or service access control, data integrity/privacy, and availability) may lead to widespread adoption of frameworks for IoT in medical area or medical based services. Such systems are fundamental to future technology. In any case, the high asset requirements of complex and heavyweight traditional security devices cannot be managed by asset-bound IoT edge computing networks, which comprise critical fundamentals of IoT-based medical care monitoring systems. Likewise, the centralization approach generally took on by the cutting edge security systems isn't well pertinent to IoT enabled medical devices with edge computing networks because of weak link issues. To wrap things up, it is beneficial to feature that regular cutting edge guard instruments can't guarantee total carefully designed frameworks for safeguarding of IoT enabled medical devices with edge computing networking. Subsequently, there is a dire requirement for novel security mechanism to address the squeezing security difficulties of medical technology enabling with IoT edge networks in a viable and effective way before they gain the trust of every single included partner and arrive at their maximum capacity in the medical services market [20]. In this specific circumstance, instruments innovation with blockchain technology has been anticipated by the business and examination local area as a troublesome innovation that can be coordinated as proper solution into novel security for IoT enabled medical instruments with edge computing networking edge computing network, as it can assume a important part as: (a) providing a high authentication services to the IoT enabled medical devices and (b) controlling unauthorized access during the transformation of data. Despite the fact that there are already a number of blockchain-based security tools actively proposed for various types of IoT edge computing networking, blockchain for IoT edge computing networking in medical technology -based security components are sorely lacking. There is hope for work on planning and improving security systems based on blockchain technology for such computing networking. Towards this direction, it is imperative to have an in-depth understanding of the following two types of blockchain-based security components at an early stage (a) the many existing ones that are explicitly intended for IoT edge computing networking in medical technology, and (b) Those that are intended for different types of IoT. However, systematically organizations in IoT edge computing networks can be taken up in medical due to comparable capabilities and distinctive qualities. Along these lines, this paper is focusing on the audit the best in the class of the over two kinds of blockchain-based security systems to give an establishment to getting sorted out research endeavors towards the plan and advancement of reliable blockchain-based countermeasures tending to the squeezing security difficulties of medical technology based on IoT edge computing networks in a viable and proficient way. It is worth focusing that we limited our attention on the combination of blockchain technology into the: (a) user authorization mechanisms, as both include the main degree of compelling security in any system, and (b) Anomaly-based Intrusion Detection Systems (AIDSs), utilizing Machine Learning (ML) methods, due to their capacity to distinguish new, beforehand obscure network attacks.

2 Literature Review

In recent technological developments, fog computing based IoT has emerged as the most used technology. Some important security approaches were not included in the previous research, which are: (a) Data transferred from medical care IoT enabled devices to cloud servers is usually decoded and easily tempered and attacked. This allows patient sensitive health related data to be publicly disclosed (ii) As far as technology adaptation is concerned IoT enabled devices in medical care are the key to identifiable proof-of-stake that allows the user to verify the data and authenticate this medical care information. This security framework can be made complete and more secure by using blockchain technology. In-detail concerns, servers must perform some tests on the network edge in a somewhat verifiable and decentralized manner. This section covers the current strategies, approaches, and calculations about being fully connected to medical services IoT, Fog, Cloud and Blockchain. These methods mainly focus on security, unbreakable quality, digital attack, IoT information verification, and IoT Gadget ID. A portion of the current chips in IoT security, blockchain and medical services, summarized as follows:

Researchers [19] proposed a core framework called BeeKeeper which is integrated with Blockchain and IoT technology. This proposed framework enables a centralized cloud server to process the data by performing calculations on the data offered by the user. In this, any node that can be considered leading to authenticate to the server is chosen by the current administrator of the framework. Researchers have used the Ethereum blockchain to deploy Bee Keeper. While the researchers, Somino et al. combined private and public key attributes used different verification processes. Users who own these combinations of attributes can use them in the verification process. Users here are individuals using IoT enabled devices. However, their proposed strategies cannot drive identifiable proof of IoT enabled devices. They have incorporated various operations of cryptographic approaches integrated with blockchain strategies in IoT to limit deferrals and streamline network traffic. Anyway, no work has been done on the adaptability issue of blockchain and IoT.

In the same research series, Resarcher [14] proposed a centralized protocol that acts partially. In this the fundamental authority was accountable for creating parameters for users and excavators. The authenticated users used attributes based on encryption schema with the goal that they could be checked and decoded by some explicit excavators and users who own the attributes. The strategy was somehow conducive to keeping up with IoT secure transmission. In any case, their proposed work does not mark the issue of gadget distinguishing proofs and verification of keys. They center on secure transmission in a concentrated manner for the most part. A communicated environment is missing in this proposed work.

Reserchер [17] used blockchain for information incorporation and secure transmission. The decoded information is usually stored away in various areas on the receiving site following a shared document storage convention. They created conventions for edge gadgets such as FCs, which help end-clients handle information while maintaining trustworthiness via the blockchain.

In any case, the existing methodology does not provide effective access control for information discovery on the blockchain in view of blockchain for patient well-being records or clinical records. As the latest research shows, blockchain is not search-adjustable; seeing a particular record will be extraordinarily delayed with information escalation. [13] A new blockchain-based human asset executive's strategy. The technology relies on the broadcast record strategy (DL). The creators depict the security protection process used to provide a straightforward framework when dealing with human asset records.

The public-private key pair was generated with an association ID, a privacy scheme, and a hash [7]. The work's exhibitions were dissected in light of the frustration point distinction proof, timing, read-write latency, and memory usage. In the interim, it performed better for all limits except the use of time. Still, the performance is high. [1] Introduced a clever intensive blockchain-based Trusted Security Savings Infrastructure (DBTPPS) to address difficulties such as security, trust, security and centralization factors. The creators attached three modules: a two-level security protection module, trust authorities, and a feature detection module [18].

The core module depends on the BC which is aggregated with an autoencoder. The reliability module is made up of the BC-based address infamous framework. The last one was remembered for its deep brain network-based approach. The location rate and accuracy of work undertaken were 93.87 percent and 98.97 percent, respectively. Anyway, they did not assess the general feasibility of the proposed approach [6]. Le et al. articulated an original method known as Underground Insect State Augmentation (ACO) for security and secure and reliable IoT information sharing; He took a multi-part support vector machine with a circular bend cryptosystem (ECC). Insurance and honesty were achieved by blockchain.

Test checks demonstrated that the work achieves superior accuracy and review and thus guarantees safety, security, confidentiality and dependability. In any case, securing the various parts of the scrambled dataset is challenging. [8] introduced an original strategy known as blockchain-based combined learning (BFL) to deal with security protections for traffic stream expectation. The creators similarly demonstrated that the strategy can be used to empower dependencies and that decentralized promotion achieves joint learning without involving an integrated model facilitator. The work provided better security insurance and prevented attacks from damaging information. However, in this method the above correspondence is a bit excessive. [4] Outlined a basic advanced trust model integrated with a multi-faceted, versatile and trust-based weighting framework. The creators introduced mathematical methods to deal with belief evaluation. The inexhaustible quality of the technology that fosters flexibility is greatest, however, as the creators didn't zero in on the control-circle idea and their coordination to complete a decentralized IoT framework. [2] Expressed a new blockchain-based Trust the Executive Instrument (BBTM) to deliver improved reliability of the Sensor Hub. The creators featured better trust assessments and checked the evaluation cycle. This work achieved improved confidence accuracy, flexibility and cohesion against attacks. Be that as it may, there is no opportunity for continuous application.

In the customary symmetric origin model, encryption is accomplished using a symmetric key. The information owner separates the information into a few assemblies and later scrambles these gatherings using a symmetric key. Clients who have private keys can interpret the scrambled information. In this scheme, the accepted customers are entered in the ACL [11]. The significant disadvantage of this scheme is that the amount of keys becomes straightforward as the number of information increases. Similarly, assuming that any change occurs between the customer and the information owner, it will affect different customers in the ACL. Accordingly, in short, this scheme is not viable for use in various situations [9]. Finextra referenced in its 2021 expected pattern for blockchain, that it is normal that the worldwide blockchain market will grow to US$39.7 billion by 2025 [10]. In 2019, Deloitte Global Blockchain Overview revealed that the industry is going through a period of growth in blockchain areas, for example, media transmission and inside fintech applications before its underlying major use [3]. Similarly, it was determined by Gartner that blockchain will generate an annual business honor of over USD 3 trillion by 2030 [16]. With these fascinating reports and patterns, there has been some interest in the adoption of blockchain in IoT-based systems. This is because IoT has had a huge market in various sectors over the years. A report by Business Insider suggests that by 2027, the IoT market will reach an annual growth of over USD 2.4 trillion [15] in a row.

With this tremendous growth, a great interest was revealed by Industry 4.0 drive to digitize modern resources. Industry 4.0 is the fourth modern upheaval that includes accompanying patterns including man-made consciousness (AI), high-level mechanization, and information testing [5]. In any case, with this massive development, there are security gambles that come into play when impacts this extended network is empowered within the basic foundation, for example, IIoT [12].

3 Proposed Methodology for Secure Authentication

Here's a high secure authenticated algorithm that allows their users to scramble next to them and transfer it to the circulating records. Through this proposed extended secure, validated computation, clients can search for watchwords anonymously using the Blockchain Client API. If the customer loses the key, they can reject the strategy and request another key. It protects against dynamic plot attacks. The details of the various limits and numerical documentation used in our proposed structure are displayed in Table 1:

In the algorithm I, characterize a technique which is based on the users' attributes-based signature technique. This proposed admittance control depends on traits and element determination. On the off chance that a client satisfies the rules in light of the necessary credits, he is given admittance, in any case, the entrance is denied. Our proposed admittance control system utilizes a half and half brain network with property based admittance control, which makes it adaptable and safer. Our proposed system comprises of four fundamental members, i.e., administrator,

Table 1 Considered parameters for the proposed algorithms

S.No.	Considered Parameters	Parameters Description
1	CID	Clinician ID
2	BN	Blockchain network
3	LID	Lab ID
4	Rs	Ring signature
5	PHR	Patient health record
6	U_{Name}	Username
7	P^K	Private key
8	R	Integer
9	N	Number of nodes
10	G	Bilinear order group
11	P^1	Generator of additive first group
12	P^2	Generator of additive second group
13	Id	Bilinear identifier
14	H	Homomorphic encryption
15	K	Degree of signature

specialist, patient, and lab expert. We propose designation strategies and calculations for every hub.

Algorithm I: Users Selected Attributes Based Signature Technique

Input: Signature ace public key $P_{pub} \rightarrow s$ of region of interest, framework boundaries parameters of area, message M_0, e's personality I_De, and advanced signature (h_0, S_0)

1. Convert the raw data values sort of h_0 to number;
2. If the event that $h_0 \in [1, N - 1]$ doesn't hold
3. Confirmation falls flat;
4. End if
5. Component $t = gh_0inG^T$;
6. Number $h = H_2(M||w, N)$;
7. Number $l = (r - h)mod\ N$;
8. If $l = 0$,
9. Go to stage 2;
10. End if
11. Number $h_1 = H_1(I_De||h_{id}, N)$;
12. Component $P = [h_1]P_2 + P_{pub} - sinG_2$;
13. Component $u = e(S_0, P)inG^T$;
14. $w_0 = ut_{in}G^T$;
15. Conversion of the data types of w_0 into a bit string;
16. Number $h_2 = H_2(M_0||w_0, N)$;
17. If $h_2 = h_0$ holds the values ***then***,
18. Check a positive outcome;
19. Else
20. The confirmation falls flat;

21. End if

Process output: Verification result: Succeed or fail (with error occurrence).

4 Proposed Algorithm for Secure Access Control

Algorithm II proposes an improved homomorphic encryption process for users, which includes setup, installation, update, and discovery steps. The arrangement step gives the design to the calculation, where the installation arrangement introduces the limitations. This section promotes the coupled illustration of Spring Search (BSS) computation. Double numbers, such as 1 and 0, indicate a double rendering of the SSA. Since prey location is discrete, each variable on the axis must be addressed by the appropriate twofold properties. Since there are only two numbers in the paired form, that is, one and zero, the position shift is characterized by adjusting the position from zero to one or from one to zero [18]. A probability ability is used to execute the possibility of being displaced in a double form. The new area of every part in every aspect of the issue may change or remain in one piece depending on the value of this potential. The probability is ID_Y, IDD_Y which becomes one or zero in the BSS calculation. In both parallel and real forms, the means are refreshed as do the amount of transfer of friendly individuals from the population. The steady fluctuations of the spring yield constant benefits of the spring [6].

A population where the difference between the two types is refreshed, where 0 and 1 are the potentials. The position below traces the space of every facet aspect. The probability of each individual from the population fluctuates in its position given the above condition. In aspect D, the higher article I denotes the probability of increasing with a higher value of $I = D_Y$. The specific circulation tracks a 0 to 1 stretch in the light of an arbitrary number. Standard abilities are seen to depict the way the ideal arrangement is viewed.

Algorithm II: Improved Homomorphic Encryption Technique algorithm

Input: Public Key

1. $T \leftarrow 0$ ordered by index values W;
2. Choose key K_S for P_{RF};
3. Choose keys K_X, K_I, K_Z f or P_{RF} F_p;
4. Z^*_p and parse DB as $(id_i, W_{idi})d_i = 1$;
5. $t \leftarrow N$;
6. $K_e \leftarrow F\ (KS, w)$;
7. *For* id ∈ DB(w) d_o
8. Counter $c \leftarrow 1$;
9. Compute $x_{id} \leftarrow F_p(K_I, i_d)$, $z \leftarrow F_p(K_Z, w||c)$;
10. $y \leftarrow x_{idz} - 1_e \leftarrow E_{nc}(K_e, i_d)$;
11. $x_{tag} \leftarrow gF_p(K_X, w)$ x_{id} and $X_{Set} \leftarrow X_{Set}$ Ux_{tag};

12. Append (y,e) to t and c ← c + 1;
13. T[w] ← t;
14. End *for*
15. $(T_{Set}, K_T) \leftarrow T_{Set}.Setup(T)$;
16. Let $E_{DB} = (T_{Set}, X_{Set})$;
17. ***Return*** E_{DB}, $K = (K_S, K_X, K_I, K_Z, K_T)$;
18. Generation of token (q('w), K);
19. Client's feedback is K and inquiry q('w = $(w_1, \ldots, w_n)$);
20. Compute $s_{tag} \leftarrow T_{Set}.GetT_{ag}(K_T, w_1)$;
21. Client sends stag to the server;
22. ***For*** c = 1, 2, … Until the server stops do
23. ***For*** i = 2, …, n do
24. $x_{token}[c,i] \leftarrow gF_p(K_Z, w_1 \| c)F_p(K_X, w_i)$;
25. ***End for***
26. $x_{token}[c] \leftarrow (x_{token}[c,2], \ldots, x_{token}[c,n])$;
27. ***End for***
28. $T_{okq} \leftarrow (s_{tag}, x_{token})$;
29. Return T ok_q;
30. Apply any sorting and searching technique;
31. $E_{Res} \leftarrow$;
32. $t \leftarrow T_{Set}(retrieve)(T_{Set}, stag)$;

Process output: Verification result: Succeed or or fail (with error occurrence).

5 Conclusion

Blockchain has probably been the most advertised innovation in the last 5 years due to the notoriety earned by the various cryptographic forms of money. Many use cases have been executed using bitcoin, Ethereum, and other blockchain innovations.

Be that as it may, none of these use cases involve infrastructure with information in the form of fragile structures and their resources. While blockchains including Ethereum highlight the importance of privacy, honesty, and reasonableness for their customers, there are significant safety and security gambles with them that have been examined and linked to their use in fundamental situations such as IoT situations in this paper. These security issues exist in other blockchains because one of their primary planning standards is the use of record propagation.

The current guide to Ethereum 2.0 contains future improvements that address the security issues examined in this paper. Nevertheless, with all the additional security and security highlights, it is important to dissect and focus on the presentation of any blockchain structure before expressing passivity in critical situations. We carried out the core comprehensive methodology of homomorphic encryption within the framework of computerized medical services, using blockchain innovations that provide a protected watchword search office at the client end. Our test strategy

maintains durability and resistance to tampering and delivers secure information, minimizing security breaks for medical services. Data addition, our core system allows blockchain clients to scramble the information next to them and transfer it to the broadcast records for record purposes in the fog environment. With homomorphic secure signature encryption technique in mind, customers can securely view ideal health information without decoding it.

In addition, it protects dynamic collaboration and repels attacks due to the sacrifice of adaptable strategy. Blockchain innovation additionally maintains circulating information, uncovers duplication, and highlights the intrinsic failures of computerized structures. In this proposed research, motion difficulties and issues in writing seen by the advanced medical services industry will be tackled. This paper proposes a set of algorithm that empowers the secure access control strategy for clients to meet the safety and security of patient well-being information in the PHR framework. The proposed technology gives customers more autonomy, and it maintains adaptability and great catchphrase search. With this proposed methodology as the most cutting-edge approach to medical services, blockchain innovation and fog computing equipped devices, further developed security and privacy in contrast to benchmark models such as Separately Medic, MedChain, and Medicaid.

References

1. Biswas, K., Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on Smart City; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), 1392–1393
2. Choo, C. W. (2002). *Information management for the intelligent organization: the art of scanning the environment*. Information Today, Inc.
3. Daraghmi, E.-Y., Daraghmi, Y.-A., & Yuan, S.-M. (2019). MedChain: a design of blockchain-based system for medical records access and permissions management. *IEEE Access, 7*, 164595–164613.
4. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018). Blockchain: a panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing, 5*(1), 31–37.
5. Feng, C., Yu, K., Bashir, A. K., Al-Otaibi, Y. D., Lu, Y., Chen, S., & Zhang, D. (2021). Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach. *IEEE Network, 35*(1), 130–137.
6. Hameed, K., Ali, A., Naqvi, M. H., Jabbar, M., Junaid, M., & Haider, A. (2016). Resource management in operating systems-a survey of scheduling algorithms. *Proceedings of the international conference on innovative computing (ICIC)*, Lanzhou, China, (pp. 2–5)
7. Hang, L., & Kim, D.-H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors, 19*(10), 2228.
8. Jung, Y., Peradilla, M., & Agulto, R. (2019). Packet key-based end-to-end security management on a blockchain control plane. *Sensors, 19*(10), 2310.
9. Kasra Kermanshahi, S., Liu, J. K., Steinfeld, R. (2017). Multi-user cloud-based secure keyword search. *Australasian Conference on Information Security and Privacy*. (pp 227–247)
10. Kasra Kermanshahi, S., Liu, J. K., Steinfeld, R., & Nepal, S. (2019). Generic multi-keyword ranked search on encrypted cloud data. *European Symposium on Research in Computer Security*, 322–343.

11. Kermanshahi, S. K., Liu, J. K., Steinfeld, R., Nepal, S., Lai, S., Loh, R., & Zuo, C. (2019). Multi-client cloud-based symmetric searchable encryption. *IEEE Transactions on Dependable and Secure Computing, 18*(5), 2419–2437.
12. Khujamatov, K., Reypnazarov, E., Akhmedov, N., Khasanov, D. (2020). Blockchain for 5G healthcare architecture. *2020 International Conference on Information Science and Communications Technologies (ICISCT)*, (pp. 1–5)
13. Kim, H., Kim, S.-H., Hwang, J. Y., & Seo, C. (2019). Efficient privacy-preserving machine learning for blockchain network. *Ieee Access, 7*, 136481–136495.
14. Malathi, D., Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., & Sangaiah, A. K. (2019). Hybrid reasoning-based privacy-aware disease prediction support system. *Computers & Electrical Engineering, 73*, 114–127.
15. Nkenyereye, L., Adhi Tama, B., Shahzad, M. K., & Choi, Y.-H. (2019). Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing. *Sensors, 20*(1), 154.
16. Rathi, V. K., Chaudhary, V., Rajput, N. K., Ahuja, B., Jaiswal, A. K., Gupta, D., Elhoseny, M., & Hammoudeh, M. (2020). A blockchain-enabled multi domain edge computing orchestrator. *IEEE Internet of Things Magazine, 3*(2), 30–36.
17. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal, 4*(5), 1250–1258.
18. Yu, B., Kermanshahi, S. K., Sakzad, A., & Nepal, S. (2019). Chameleon hash time-lock contract for privacy preserving payment channel networks. *International Conference on Provable Security*, 303–318.
19. Zhou, L., Wang, L., Sun, Y., & Lv, P. (2018). Beekeeper: a blockchain-based iot system with secure storage and homomorphic computation. *IEEE Access, 6*, 43472–43488.
20. Parag, V., Rajeev, T., Wei-Chiang, H., Shuchi, U., Yi-Hsuan, Y. (2022). FETCH: A deep learning-based fog computing and Iot integrated environment for healthcare monitoring and diagnosis. IEEE Access 1012548-12563 9682727. https://doi.org/10.1109/ACCESS.2022.3143793