International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

An Adaptive Blockchain based Three-Tier Architecture in Fog based IoT for Personal Healthcare Data Application

J.N.S.S Janardhana Naidu [*1], E.N Ganesh[2]
[1]Department of Computer Science and Engineering,
Vels Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu 600117, India.
Email: jnss.janardhana@gmail.com
[2]Department of Computer Science and Engineering,
Vels Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu 600117, India.
Email: enganesh50@gmail.com

Abstract: To protect patient health data (PHD) and ensure the security of healthcare IoT devices, this paper presents an Advanced Signature-Based Encryption algorithm (ASE), a blockchain analytical model, a mathematical framework, and an Adaptive Fog Computing based Three-tier Architecture (AFCTTA). The aim is to enable safe access to real-time services and IoT for end users. This AFCTTA was constructed on a blockchain platform, providing trustworthy data transmission between patients, clinicians, fog nodes, and IoT. Additionally, a decentralized fog computing-based blockchain analytical model along with a mathematical framework were produced to ensure secure transfer of data and transactions within healthcare IoT. To ensure secure communication between devices and fog nodes, a private block chain was implemented in order to validate certificates and keys. As an added security measure, an ASE method was devised. This algorithm utilizes War Optimization Strategy (WOA) to select optimal keys for securing data from heterogeneous and homogeneous IoT healthcare equipment. Through its encryption process utilizing various cryptographic techniques, all traffic is encrypted before being decrypted once it reaches its intended destination. To validate its proposed approach, UCI machine library is collecting health care data. To execute this method, Python is utilized and compared to traditional algorithms such as Rivest-Shamir-Adleman (RSA), Elliptical Curve Cryptography (ECC), and Tiny Lightweight Symmetric Encryption-Aquila Optimization Algorithm (TLSE-AOA).

Keywords: Digital signature, Patient Health data, Advanced Signature-based Encryption, war optimization strategy, Blockchain technology

I. INTRODUCTION

Fog computing is another innovation that supports the cloud and expands the management of distributed computing closer to end gadgets. The cloud is usually located far away from the gadgets that use their administrations, and part of the new research suggests that combining a fog server with light middleware will overcome any barriers and provide rich assets near the end gadgets [1]. Security is an urgent element for proper work of fog computing. In particular, stabilization and key trade-offs are major difficulties to be considered in fog computing. Guaranteeing secure shared authentication is vital to the security of fog processing. Be that as it may, current common verification schemes have huge computational overheads or cannot perform secure shared verification [2].

The fog figure is positioned in the middle of the cloud and IoT devices to satisfy the criteria indicated above [3]. So, in addition to the traditional cloud-IoT engineering, fog computing layers provide another layer. IoT applications have been discussed in several academic publications and cutting-edge studies over the last few years. These decisions and assertions lead logically to the conclusion that IoT applications need a high response rate and consistent quality. Additionally, IoT applications need a lot of processing power and storage space owing to the increasing rate [4]. Fog computing was developed for many of these reasons, and it was just as essential as cloud computing a short time ago [5]. However, such convergence between IoT and fog computing is not without costs; Some difficulties influencing effective implementation of fog detection are enumerated. These difficulties are largely depicted as being linked to correspondence performance (network difficulties) and security and safety challenges [6]. Also, fog log implementation information, energy usage, IoT controlled assets (e.g., power and memory management) and may face various problems related to long-term network [7].

The world's fastest expanding industry may be that of medical services. Here, it views the healthcare business as a multidimensional body that oversees a number of industries, including education, manufacturing, pharmaceuticals, banking, travel, and information technology [8]. Nearly all management

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

organizations in the medical services industry are public, semi-public, or private. Medical care offers both patients and laypeople a variety of help by functioning under these kinds of integrated systems. The medical services sector is setting up job openings in IT and non-IT areas, carrying out innovative work to develop new creative products and administrations, enabling the training sector by providing equitable assistance, creating companies for medical devices and pharmaceutical manufacturers [9]. Producer helps telemedicine producer, healthcare providers, travel industry and more. A number of papers have been presented of late, as part of this blockchain reception, which guarantees that blockchain is one of the best means of identifying safety and security challenges. Be that as it may, the writing in this space is very different [10].

The rest of the article has been organized as follows, with section 2 offering pertinent research on security in fog computing. The detail explanation of the projected technique is explained in the section 3. The outcomes are explained in the portion 4. The summary of the paper is presented in the portion 4.

II. RELATED WORKS

Various techniques are available to achieve the security in fog computing architecture. Few works are reviewed in this portion.

A blockchain-enabled federated learning (FL-Block) system has been presented by Youyang Qu *et al.*, [11] to narrow the gap. With a blockchain-based global learning paradigm, FL-Block enables neighbourhood learning updates of trade end devices, as certified by miners. Based on this, FL-Block organises autonomous AI via the blockchain utilising a proof-of-work contract structure, empowering it to pursue a global model with almost no centralised state.

Abdullah Al-Noman Patwary *et al.*, [12] have introduced a secure decentralized area-based gadget-to-gadget verification model, in which hash gadgets can verify each other in a mist layer, typically using blockchain. Here, the fog gadget contemplated the Ethereum Blockchain stage for admission, verification, confirmation and information storage. Here, general framework engineering, different members and their exchanges and message communication between members are introduced.

Using an elliptic curve cryptographic (ECC) computerised signature, Desire Ngabo *et al.* [13] have developed a public permissioned blockchain security tool that uses a distributed registry data set (employee) to offer directness, patient protection, and an immutable security arrangement. In the IoT's fog layer, logs alter. The fog model's problems with inertia, centralization, and flexibility are lessened by the blockchain discovery technique. The ability of information in the diagnostic layer (human wearable gadget) and cloud data set IoT has led to the development of security countermeasures against medical information mining concerns, which is a main focus of this work (IoT).

A security governance engineering supported by blockchain and hash processing that operates on edge fog centres assembling hardware clusters has been presented by Tharaka Hewa *et al.*, [14]. The suggested administration maintains anonymity and non-reproducibility on the blockchain while using cloud production hardware verification and gear cloud channel security insurance. Here, the recommended engineering was put into practise using a Hyperledger system, and the presentation benefit over more complex arrangements was examined.

In order to safely verify clients, Otuekong Umoren *et al.* [15] have developed a verification framework that makes use of the features and advantages of blockchain technology as well as interesting contracts. The architecture in place uses the client's email address, username, Ethereum address, password, and biometric accountant information for registration and verification. Experiments demonstrate that the suggested approach was safe, and the implementation improvement was achieved in comparison to the ways already in use.

III. PROPOSED SYSTEM MODEL

Figure 1 illustrates an innovative, three-tier architecture incorporating fog computing and blockchain technology in healthcare IoT networks. This approach adds a fog layer between one comprising of IoT devices and cloud data centers. This layer consists of blocks, ledgers, smart contracts written using computer language, as well as decentralized apps to connect with healthcare IoT. Equally significant is that this single-hop count enables easy access for both patients and medical experts to use this fog layer. Cryptographic operations are used at edge of these networks to maximize security afforded by FC notion and blockchain method adopted here.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

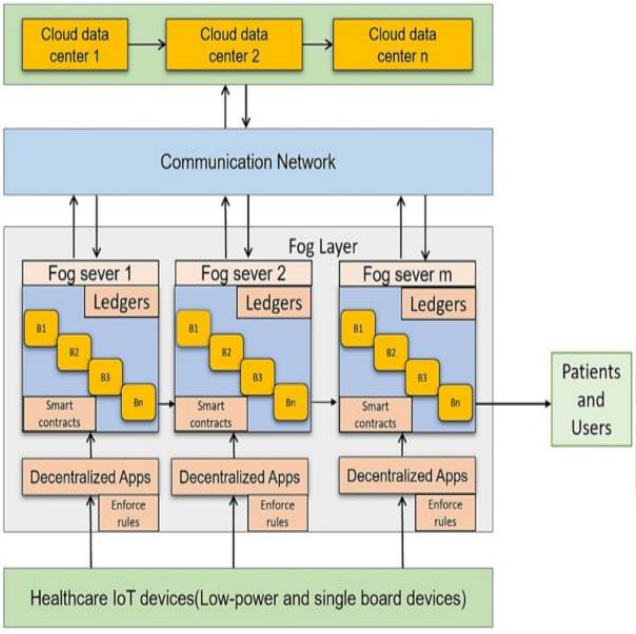

Figure 1: Three-tier architectures

Creating a secure system model for healthcare IoT communication, data authentication, and device identification necessitates an architecture that meets real-world implementation needs. Examining cutting-edge technologies reveals healthcare IoT lagging behind three-tier FC blockchain architecture in development and QoS requirements. Analytical models such as Femto Cloud, FogBus, BFAN, and Beekkeeper were not specifically designed to meet healthcare IoT demands and are therefore inadequate to ensure a secure channel of exchanging critical data.

A. Blockchain technology

Blockchain technology plays a notable role in many aspects of modern applications, including ad hoc networks, fog networks, cloud and edge computing, the internet of things, bitcoin, and more. This is due to its ability to provide automatic peer-to-peer connectivity; reducing the chance of single-point failure. Distributed ledger systems are used as part of this task to keep costs low while allowing complete anonymity. To begin with it was Bitcoin that first put distributed timestamp servers and blockchains together. The main objective being to computationally demonstrate a chain of digital signatures [17]. As illustrated in Figure 2 a typically structured Bitcoin block consists of two components: a parent block and an earlier block hash - making up what is known as the 'block header'. In reality any number of blocks may be included on the Ethereum network using the hashes from their predecessors.

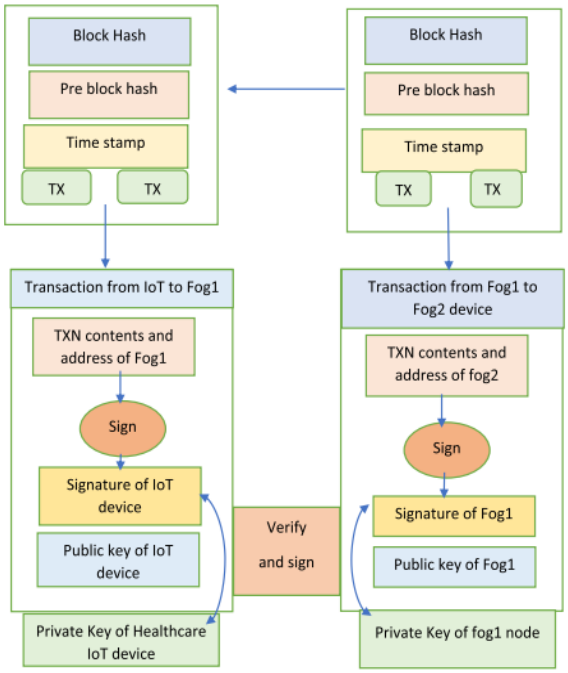

Figure 2: Blockchain technology

This framework concept includes wearable devices for patients and professionals as well as medical care IoT entities, FC inventories, smart contracts, and medical care IoT devices. Assign healthcare data to hash hubs and knowledgeable fog servers rather than passing it via blockchains and cloud servers. Fog storage medical services group PHD created by IoT devices into comparable blocks connected to a certain block. Fog nodes are connected to IoT for healthcare. The system includes fog centres and IoT devices for medical services, and they must use their own credentials, notice confirmation, and key exchange to prove the validity of the devices and information. When the proof of PHD information verification and identifying medical care IoT devices is finished, the transfer of the information is meticulously stamped with a ring signature. Here, the fog centres are gathered in one place. The master fog node of each cluster has a public key. Depending on the necessity for keys and exchanges, the roles of fog nodes and professional fog centers may alter. Ace has a centre that chooses receivers of PHD medical care IoT devices according on the needs of customers and patients. Key and PHD requests are also handled by them. In order to ensure secure transmission of PHD documents between medical service IoT devices and relevant specialist or medical institutions, a specific framework is employed. This entails first sending documents to a hash server to be verified with a digital signature before transmitting it through an IoT network. This signature and its associated public key must be confirmed by a master fog center in order for processing of said documents to continue safely. In case verification is unsuccessful, alternate hubs step in and take over instead, as

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

Haze Hub will not send any medical care IoT data that could not be validated by either computerized ring signature or its public key.

B. Advanced Signature-Based Encryption

Ingenious cryptographic methods like Diffie-Hellman key swapping and enhanced signature employing blockchain technology are combined in the recently revealed ASE computation. Three phases make up the advanced token for this calculation. 1) Key generation 2) Produce a token using a hash code; 3) confirm the signature. The markings are also combined to create a ring. Fog computing is a concept that deals with computation in order to safely provide patients and professionals access to time-sensitive healthcare IoT data [18]. Fog computing centers keep track of interactions between end users and IoT. Blockchain is a decentralized means of information sharing that is employed in IoT for medical services. In Figure 3, the ASE procedure is shown.

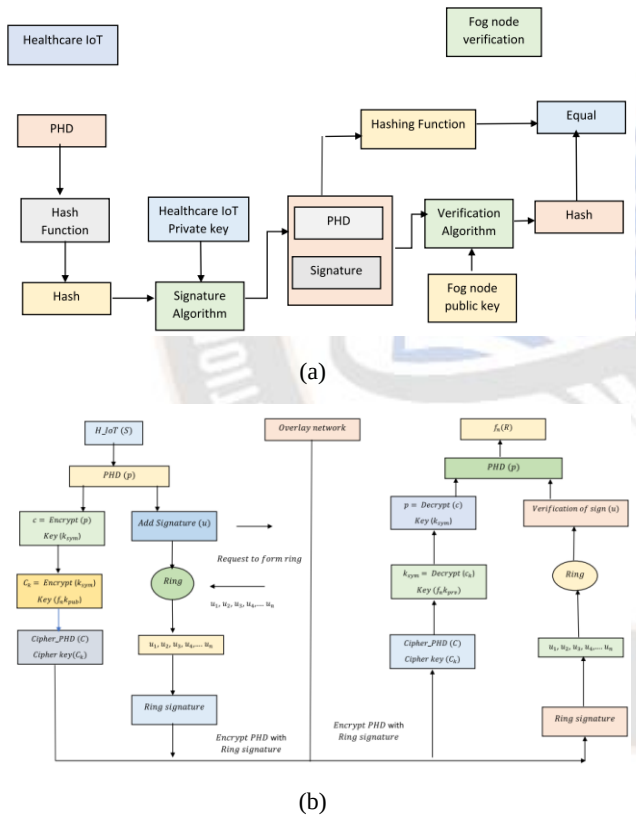

Figure 3: Analysis of (a) digital signature and (b)encryption process

In order to ensure the safest possible transmission of PHD, the algorithm is broken into four distinct parts. Firstly, a blockchain-based technique is utilized for PHD security. Secondly, Diffie-Hellman data encryption provides additional protection for healthcare IoT blockchain devices. Thirdly, authorization and verification processes must be undertaken before PHD can be transmitted. Finally, users will benefit from ASE decryption algorithms which allow them to receive their PHD safely. This ASE approach utilizes fog computing and blockchain technology to provide high levels of security and PHD dependability when handling a large volume of service requests from healthcare clients. Specifically, it is especially beneficial for time-sensitive real-time IoT healthcare operations and services that current state-of-art techniques cannot manage completely. Although there have been attempts at using similar models and algorithms in practical contexts, none have yet been as successful as this one.

C. War Optimization Strategy

By means of WOA's aid, the key is picked in the ASE. All contenders have a fair shot at emerging victorious and becoming a ruler or strong figure in every cycle dependent on their proficiency in combat (well-being value). Like two leading runners on the battleground, both commander and king step ahead together. In the arena of fight, an Officer and Lord appear to direct other contestants. An adversary warrior (near optima) who is able enough to outwit the avantgarde may engage either lord or lieutenant in fierce battle [19]. Warriors use both their strategies for development as well as the state of affairs concerning the de facto captain or ruler to evade such confrontation.

Fitness Evaluation

In the suggested organisation, the optimal key for the encryption process is selected using the WOA. The fitness feature was created to make the encryption process more robust. The random key parameters used in the fitness evaluation are used to choose the minimal encryption time-based key. An explanation of how the fitness of this system is determined is provided below:

$$FF = Min(encryption\ time) \quad (1)$$

In order to engage in search optimization during a battle, the fitness function should be reordered from small to large and every encrypted image within the cell array must be sorted. This process is illustrated in Figure 4 through a flowchart. By taking such measures, an individual has the capacity to shift the directions of their war strategy.

Attack Strategy

Algorithms for binary collisions have been presented. Generally speaking, each fighter shifts its position based on where the administrator and the ruler are. The Lord is awaiting the right moment to unleash a crushing attack on the enemy. The best offensive or physical officer is thus considered as being in charge.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

$$X_I(t+1) = X_i(t) + 2 \times \rho \times (c-k) + RAND \times \left(w_i \times k - X_i(t)\right) \quad (2)$$

In this case, k may be described as the king location, c as the leader's previous location, $X_I(t+1)$ as a novel position, and w_i as the mass.

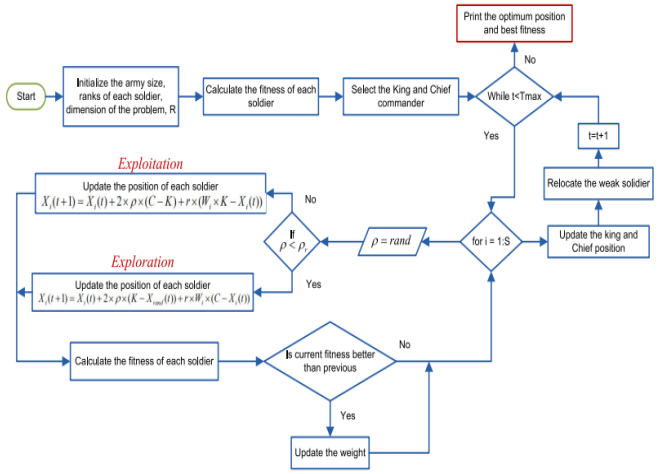

Figure 4: An outlined process of the suggested approach

Rank and weight Updation

The commander and commandant have provided a status update for all search experts, which takes into account the location and combat performance of every soldier. These elements, in combination with prevailing conditions, ascribe a weighting factor $w_i$to the individual. This information tells us how close the trooper is to achieving their desired health rate

$$(t+1) = X_I(t+1) \times \left(f_n \geq f_p\right) + X_I \times \left(f_n < f_p\right) \quad (3)$$

The soldier is regarded as the prior location when comparing the suitability of the new position $f_n$to that of the previous one f_p. The soldier's rank R_i is raised if they enhance the site successfully.

$$R_I(t+1) = (R_I + 1) \times \left(f_n \geq f_p\right) + R_I \times \left(f_n < f_p\right) \quad (4)$$

The new weight may be calculated in relation to the rank as follows:

$$w_i = w_i \times \left(1 - \frac{R_I}{Maximum\ iteration}\right)^a \quad (5)$$

Defense method

The Lord, Warlord, and Irregular Troops' levels determine the next tech level improvement. Although the arrangement and weight of the remaining components are new.

$$X_I(t+1) = X_i(t) + 2 \times \rho \times (c - Xrand(t)) + RAND \times (w_i \times c - X_i(t)) \quad (6)$$

Compared to the previous phase, this fight style explores a larger hunting area since an arbitrary combatant's position is used. The warriors make big gains and enhance their circumstances for significant improvements Wi. When they update the status, Wi Warriors makes tiny improvements.

Spare/transfer of weak sold

Sort the fighter with the worst fitness for each priority,

$$X_w(t+1) = LB + RAND \times (UB - LB) \quad (7)$$

The weaker fighter is then brought closer to the centre of a fully equipped army on the battlefield. This technique also restores the computation's assembly performance.

Exploration and Exploitation

All metaheuristic processes for constructing an assembly incorporate two vital steps - Dual Contract and Query (for Global Optima). These two stages are critical to the performance of the optimization process. The computation would be more robust if these two factors could be reasonably balanced. The investigation is addressed by the manufacturing attack procedure and the double handling defensive method. The following list of the WOA's common benefits is provided.

- The computation that is being suggested strikes a fantastic balance between exploitation and exploration.
- Each officer's (provision) intriguing weight is based on his/her position.
- Each fighter's weight is updated during the refresh process, providing they are successfully improving their health. In this manner, a molecular location in relation to lords and lordship is absolutely necessary for weight regeneration.
- Loads fluctuate nonlinearly. During the first stress, the loads fluctuate in significant steps, and during the final cycles, they vary in smaller steps. This encourages quick compounding for the highest value worldwide.
- There are two steps in the cycle of stage regeneration. It additionally strengthens the ability to do research for the optimum worldwide arrangement. Simple and requiring minimal computing effort is the suggested computation.

On the basis of this algorithm, the best encryption is accomplished. Calculate the ideal key for each encrypted data; in this case, the most effective encryption method produced the most effective encrypted data, which was then output together with the positional information needed for later decoding.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

IV. OUTCOME EVALUATION

To analyze the usefulness of the proposed approach, a laptop with an Intel Core i5-2450M CPU running MATLAB R2016b at 2.50GHz and 6GB of RAM was used to implement the technique. Table 1 presents the parameters utilized for this method. By employing metrics such as encryption, decryption, waiting, and processing times performance indicators were collected to investigate its potential when compared to RSA and ECC algorithms. The input data is sourced from UCI machine library [20]. Through these tests it was confirmed that the suggested solution effectively secures fog computing networks.

Table 1: Proposed method parameters

S. No	Method	Description	Value
1	Proposed Method	Number of IoT devices	100
2		File size	5MB
3		Number of iterations	100
4		Number of populations	50
5		Upper bound	10
6		Lower bound	-10
7		Probability factor	0.5

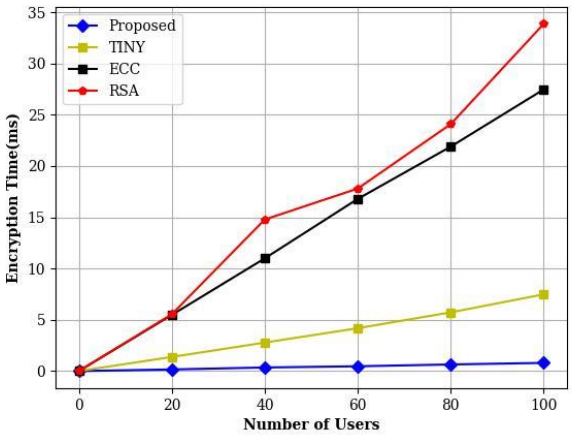

Figure 8: Encryption time versus users

An examination of encryption time and user numbers is illustrated in Fig. 4. This proposed approach is compared to established methods Tiny, RSA, and ECC. It was determined that the predicted approach achieved a 0.1ms response time for 20 users in the fog network; whereas, it took Tiny, RSA, and ECC 1 ms, 7 ms, and 5 ms respectively to provide identical performance with a single user of 20. Intriguingly enough 40 users in the fog network had an encryption time of 0.4ms using the projected approach while similar results were attained with 3 ms, 10 ms, 15 ms with Tiny, RSA, ECC and 40 users respectively. An analysis of 60 users confirmed the foreseen method had a quick encryption time at 0.5ms while its counterparts obtained equivalent results in 4 ms (Tiny), 16 ms (RSA), 18 ms(ECC). In figure 5 shows that the performance analysis of decryption time versus users has been illustrated.

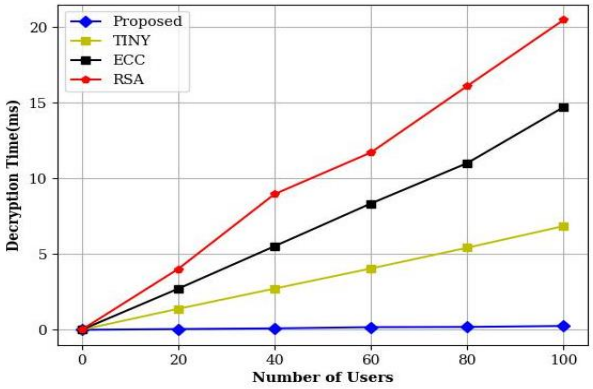

Figure 5: Decryption time versus users

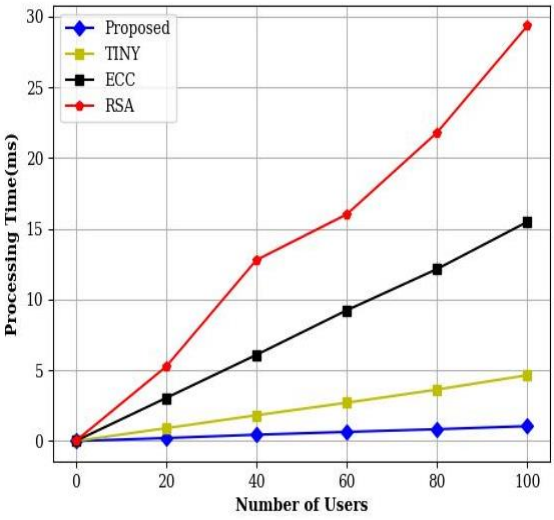

Figure 6: Processing time versus users

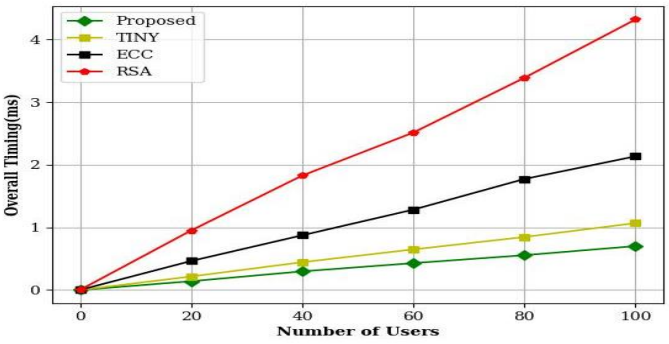

Figure 7: Waiting time versus users

Figure 6 compares the processing times of the proposed technique, TINY, ECC, and RSA in various miners. The graph demonstrates how much less processing time is used by fog nodes than by clouds. The findings showed that the suggested method performed better in terms of processing times in the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

FC environment. The methodology for comparing processing times is tested on three distinct combinations of departing methods at various miners. The comparative study of waiting time versus users is presented in figure 7.

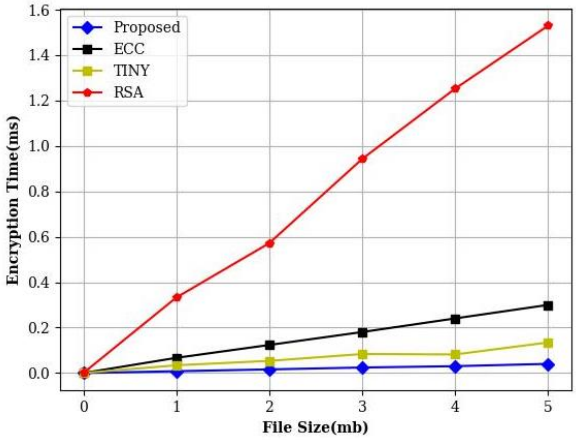

Figure 8: Encryption time versus file size

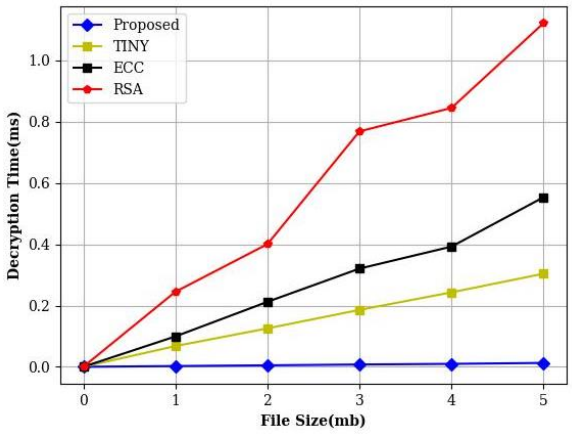

Figure 9: Decryption time versus file size

Based on their strength and file size, RSA, ECC, TINY, and suggested algorithms are compared in Fig. 8. There are a number of security algorithms utilized with IoT devices, however Fig. 8 suggests that the suggested method is most suited for IoT system security. The comparative study of decryption time vs file size is shown in figure 9. Here, the suggested approach takes 0 to 0.1 milliseconds, TINY takes 0.3 milliseconds, ECC takes 0.58 milliseconds, and RSA takes 1.18 milliseconds. The data clearly show that the suggested algorithm-based decryption is slower than the decryptions using TINY, ECC, and RSA.

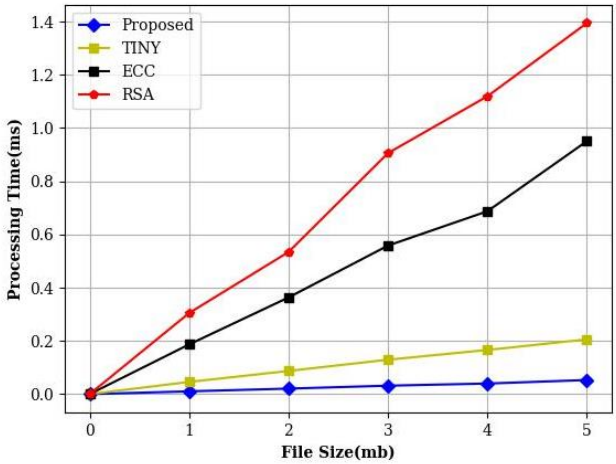

Figure 10: Processing time versus file size

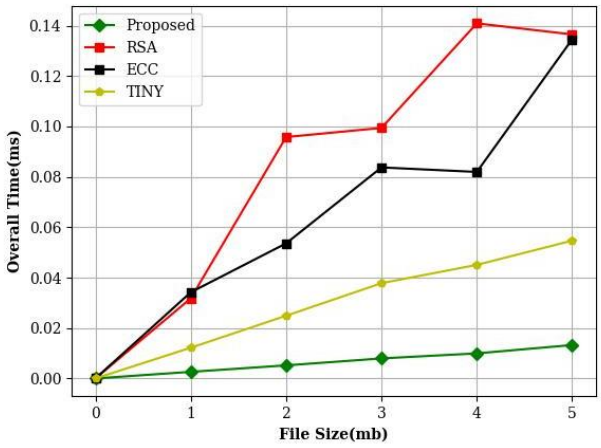

Figure 11: Waiting time versus file size

Figure 10 displays the quantity of files handled in fog and clouds together with the processing times for those files. The graph demonstrates how much faster file size processing occurs in fog nodes than in the cloud. The suggested method for healthcare IoT in FC and cloud has a 0.1 millisecond minimum processing time. The acquired processing time results showed that the suggested algorithm performed better in the FC environment when compared to other approaches like TINY, ECC, and RSA. Figure 11 illustrates the comparative study of waiting time vs file size. Here, the outcome suggests that total times increase with increasing security measures, and the simulation suggests that it almost exactly the same for different file sizes. From the above figure we can clearly understand that the proposed algorithm has better performance compared to other conventional methods like TINY, ECC and RSA.

V. CONCLUSION

The identification, verification, and PHD authentication of healthcare IoT devices are presented in this research using AFCTTA, a theoretical framework, an ASE algorithm, and an

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7786
***Article Received**: 10 April 2023 **Revised**: 18 June 2023 **Accepted**: 01 July 2023*

analytical model. Promoting safe data transfer for end users of real-time services in healthcare and IoT was the objective. The recommended idea and algorithm have shown success in providing secure services for close-to-the-edge transaction and transmission. Additionally, a brand-new ASE algorithm was devised and constructed. The technique recognises heterogeneous and homogeneous IoT medical equipment, verifies data sources and targets, and authenticates data sent through a variety of IoT devices and fog nodes. WOA is used by the algorithm in the ASE technique to choose the optimal key. Several cryptographic methods and a private blockchain are used to encrypt and decrypt the data. In order to validate the suggested method, health care data are collected using the UCI machine library. The proposed approach is implemented using Matlab and compared to more well-known techniques as TLSE-AOA, ECC, and RSA. The evaluation reveals that the proposed technique has resulted in successful outcomes.

REFERENCES

[1] Y.I. Alzoubi, A. Al-Ahmad, A. Jaradat, "Fog computing security and privacy issues, open challenges, and blockchain solution: An overview". International Journal of Electrical & Computer Engineering vol. 11, no. 6, pp. 2088-8708, 2021.

[2] Y. Liu, J. Zhang, J. Zhan, "Privacy protection for fog computing and the internet of things data based on blockchain". Cluster Computing, vol. 24, pp. 1331-45, 2021.

[3] P. Kumar, R. Kumar, G.P. Gupta, R. Tripathi, "A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing". Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, pp. e4112, 2021.

[4] M.S. Eddine, M.A. Ferrag, O. Friha, L. Maglaras, "EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles". Journal of Information Security and Applications, vol. 59, pp. 102802, 2021.

[5] A.W. Kiwelekar, P. Patil, L.D. Netak, S.U. Waikar, "Blockchain-based security services for fog computing". Fog/Edge Computing for Security, Privacy, and Applications, pp. 271-90, 2021.

[6] M. Kong, J. Zhao, X. Sun, Y. Nie, "Secure and efficient computing resource management in blockchain-based vehicular fog computing". China Communications, vol. 18, no. 4, pp. 115-25, 2021.

[7] J. Ofulue, M. Benyoucef, "Data monetization: insights from a technology-enabled literature review and research agenda". Management Review Quarterly, pp. 1-45, 2022.

[8] D. Garg, K.K. Bhatia, S. Gupta, "A Research Perspective on Security in Fog Computing Through Blockchain Technology. InArtificial Intelligence and Sustainable Computing for Smart City: First International Conference, AIS2C2 2021, Greater Noida, India, March 22–23, 2021, Revised Selected Papers" 1 2021, Springer International Publishing pp. 91-104, 2021.

[9] R.T. Hasan, S.Y. Ameen, "Security Enhancement of IoT and Fog Computing Via Blockchain Applications." Journal of Soft Computing and Data Mining, vol. 2, no. 2, pp. 26-38, 2021.

[10] V.K. Quy, N.V. Hau, D.V. Anh, L.A. Ngoc, "Smart healthcare IoT applications based on fog computing: architecture, applications and challenges." Complex & Intelligent Systems, vol. 8, no. 5, pp. 3805-15, 2022.

[11] Y. Qu, L. Gao, T.H. Luan, Y. Xiang, S. Yu, B. Li, G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing." IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5171-83, 2020.

[12] A.A. Patwary, A. Fu, S.K. Battula, R.K. Naha, S. Garg, A. Mahanti, "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain." Computer Communications, vol. 162, pp. 212-24, 2020.

[13] D. Ngabo, D. Wang, C. Iwendi, J.H. Anajemba, L.A. Ajao, C. Biamba, "Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things." Electronics, vol. 10, no. 17, pp. 2110, 2021.

[14] T. Hewa, A. Braeken, M. Liyanage, M. Ylianttila, "Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing." IEEE Transactions on Industrial Informatics, vol. 18, no. 10, pp. 7174-85, 2022.

[15] O. Umoren, R. Singh, Z. Pervez, K. Dahal, "Securing Fog Computing with a Decentralised User Authentication Approach Based on Blockchain." Sensors, vol. 22, no. 10, pp. 3956, 2022.

[16] S. Shukla, S. Thakur, S. Hussain, J.G. Breslin, S.M. Jameel, "Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model." Internet of Things, vol. 15, pp. 100422, 2021.

[17] D. Ngabo, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C, "Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things." Electronics, vol. 10, no. 17, pp. 2110, 2021.

[18] A. Mehbodniya, J.L. Webber, R. Neware, F. Arslan, R.V. Pamba, M. Shabaz, "Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data." Expert Systems, vol. 39, no. 10, pp. e12978, 2022.

[19] T.S. Ayyarao, N.S. Ramakrishna, R.M. Elavarasan, N. Polumahanthi, M. Rambabu, G. Saini, B. Khan, B. Alatas, "War strategy optimization algorithm: a new effective metaheuristic algorithm for global optimization." IEEE Access, vol. 10, pp. 25073-105, 2022.