BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

ORIGINAL RESEARCH

Secure and Reliable Fog-Enabled Architecture Using Blockchain With Functional Biased Elliptic Curve Cryptography Algorithm for Healthcare Services

Charu Awasthi, PhD Student[1]; Satya Prakash Awasthi, PhD[2]; and Prashant Kumar Mishra, PhD[3]

[1]Research Scholar Department of Computer Engineering Poornima University, Jaipur, India; [2]Associate Professor, Department of Computer Engineering, Poornima University, Jaipur, India; [3]Associate Professor, Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur, India

Corresponding Author: Charu Awasthi, Email: charuawasthi@gmail.com

DOI: https://doi.org/10.30953/bhty.v7.347

Keywords: blockchain, FB-ECC, fog computing, functional biased elliptic curve cryptography algorithm, galactic bee colony optimization algorithm, GBCOA, healthcare services

Abstract

Fog computing (FC) is an emerging technology that extends the capability and efficiency of cloud computing networks by acting as a bridge among the cloud and the device. Fog devices can process an enormous volume of information locally, are transportable, and can be deployed on a variety of systems. Because of its real-time processing and event reactions, it is ideal for healthcare. With such a wide range of characteristics, new security and privacy concerns arise. Due to the safe transmission, arrival, and access, as well as the availability of medical devices, security creates new issues in the area of healthcare. As an outcome, FC necessitates a unique approach to security and privacy metrics, as opposed to standard cloud computing methods. Hence, this article suggests an effective blockchain depending on secure healthcare services in FC. Here, the fog nodes gather the information from the medical sensor device and the data are validated using smart contracts in the blockchain network. We propose a functional biased elliptic curve cryptography algorithm to encrypt the data. The optimization is performed using the galactic bee colony optimization algorithm to enhance the procedure of encryption. The performance of the suggested methodology is assessed and contrasted with the traditional techniques. It is proved that the combination of FC with blockchain has increased the security of data transmission in healthcare services.

Submitted: August 7, 2024; Accepted: October 4, 2024; Published: December 31, 2024

Recent breakthroughs in electronic communication have altered the Internet-of-Things (IoT) with the creation of small appliances that utilize and control the gathering and sharing of information. These permit the creation of tiny, cost-efficient, and less powerful multifunctional sensing systems possessing the capability to observe and convey different data in numerous areas, including transportation, healthcare, and industry.[1]

The healthcare IoT provides several advantages, including data transfer in real-time mode and the capability to control the physiological status of the patients for varied durations. Equipment, including glucose meters, electroencephalography, electromyography wearable devices, etc., permits health providers to gather a patient's health data locally and create a decision depending on the health of the patient's information.

Clinics have been implementing the IoT for several years, and now they have healthcare IoT appliances in patient care rooms and their systems. However, clinical agencies, clinics, and corporations do not address the protection threat of healthcare IoT that is linked to a local area network or a wide area network. The IoT devices are readily hijacked, and this can lead to various concerns owing to weak validation and encoding techniques.

Therefore, blockchain is launched for safe and trustworthy transfer in healthcare IoT. Figure 1 demonstrates the framework of fog computing (FC).

The development of IoT systems, especially in the healthcare industry, is generating massive quantities of information, which are transported and saved on the cloud. Due to the need for real-time information processing and storage, handling such large amounts of cloud-based information creates a bottleneck.

The protection of information in the cloud is also a significant issue.[2] The FC idea was an attempt to solve the issue. Fog computing is a cloud computing system extension. Accompanying the cloud's functioning is fog's primary role. For example, Fog delivers computational resources to devices that are nearer to the edge of the network. The typical IoT cloud framework has problems with scalability and dependability, but FC fixes such problems.

Because fog nodes operate at the edge of the network and are more geographically dispersed, as shown in Figure 1, they improve information protection and precision, as well as minimize delay, which is critical for applications such as medical information. The total bandwidth to the cloud is also minimized, resulting in improved service quality. Healthcare IoT device detection, validation, and verification in a decentralized context may be solved by integrating FC with blockchain.[3] To address this, we present a fog-enabled architecture using blockchain with a FC, functional biased-elliptic curve cryptography (FB-ECC) algorithm for healthcare services.

Related Work

This article proposes a FB-ECC algorithm for data encryption, with optimization accomplished by the galactic bee colony optimization algorithm (GBCOA). This algorithm is compared with various algorithms proposed in different articles for its performance analysis.

Table 1 presents top line observations from researcher regarding related observations of fog-enabled architecture. The related literature summaries suggest that integration of fog architecture with blockchain utilizing capabilities of IoT devices is an interesting domain if we can incorporate a suitable algorithm for proper working.

Ngabo et al.[4] stated that the primary goal of their work is to develop protection mechanisms against medical data mining attacks created by the sensing layer and information storage in the cloud database of the IoT. A public-permission blockchain protection process that uses ECC digital signatures to assist a dispersed ledger database (server) to give immutable protection and transfer clarity as well as to protect patient information tampering at the IoT's fog layer.

Baniata and Kertesz[5] presented a thorough literature analysis and categorization of the FC-block chain (FC-BC) combination—the current state of the art of the FC-BC combination. The authors discuss and organize the relevant work based on the publishing year and area, as well as the algorithms employed, BC functions, and BC position in the FC architectural design. Investigations, evaluations, and future difficulties for the BC-FC combination are presented in detail by the author.

Tariq et al.[6] attempted to address the issues of future digital infrastructure protection at a time when it is still under development. The functionality-dependent fog framework is established with the arrival of the architecture that generates large amounts of information.

Also discussed are the need for additional protection of fog-enabled IoT devices, as are FC protection challenges and large information confidentiality related to fog-enabled IoT. Then, consideration of the complementary

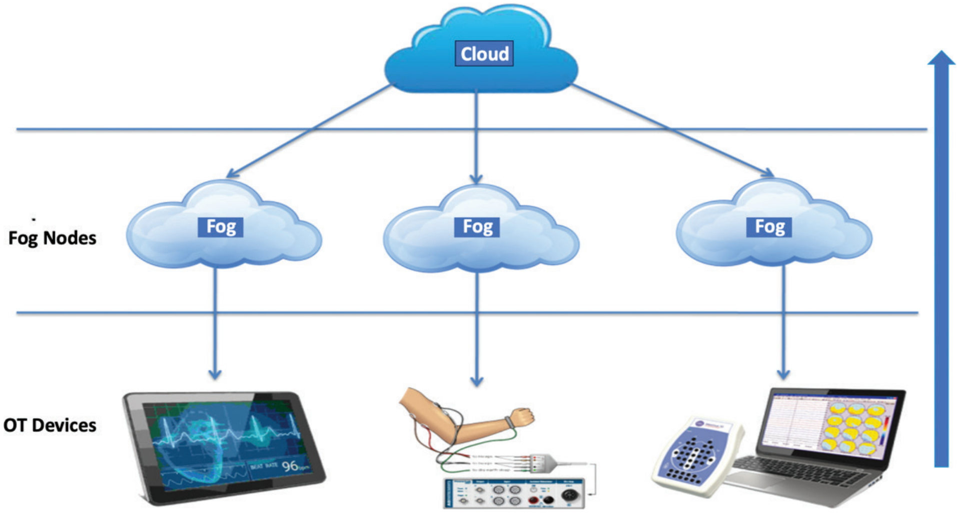

Fig. 1. Fog computing architecture.

Table 1. Observations by researchers in the field of fog-enabled architecture

Source	Top line observation
Ngabo et al.[4]	The primary goal is to develop protection mechanisms against medical data mining attacks created by the sensing layer and information storage in the cloud database of the IoT.
Tariq and colleagues[6]	Address issues related to future digital infrastructure protection.
Banerjee et al.[7]	Enhanced user experience and service resiliency in the event of an emergency.
Fernández et al.[8]	Implemented a system that adds IoT capabilities to the commercial CGM to enable remote surveillance of patients.
Muthanna et al.[9]	Proposed a framework for SDN to regulate and manage an edge computation layer of fog nodes.
Srivastava et al.[10]	Discussed FC, blockchain, and the IoT in healthcare
Yánez et al.[11]	Suggested a new context-aware approach for on-chain information allocation in IoT-blockchain networks.
Kumari et al.[12]	Provided an examination of the functions of fog and cloud computing and the IoT in providing continuous context-aware services to end users.
Pareek et al.[13]	Observed that IoT links many gadgets globally.
Hanumantharaju et al.[14]	States that IoT might help patients and healthcare providers keep in touch and offer their community clear, value-dependent care.
Mayer et al.[15]	Proposed a FC architectural paradigm that integrates blockchain, fog computing, and the IoT for the healthcare area.

FC: fog computing; CGM: continuous glucose monitoring; IoT: Internet of Things; SDN: software-defined networking.

interdependencies between blockchain and FC, as well as their role in addressing a wide range of protection concerns in IoT, are discussed. As a consequence, this study offers a taxonomy of the kinds of attacks on fog-dependent IoT systems, compares the most recent contributions to the area in terms of their protection service, and makes recommendations for future research.

Banerjee et al.[7] enhanced the user experience and service resiliency in the event of an emergency; FC techniques have been utilized to link IoT with real-time computation at edge networks. Fog edge computing, with its dispersed design and proximity to end-users, may deliver quicker reaction times and higher quality services for IoT use. FC, IoT, and machine learning are included in every part of the paradigm provided by the researchers to improve the quality of healthcare. Blockchain technology is used to assure architecture protection.

Fernández et al.[8] implemented a system that adds IoT capabilities to the commercial continuous glucose monitor (CGM) to enable remote surveillance of patients and, therefore, notify them of potentially hazardous circumstances. To gather CGM blood glucose measurements, cellphones are used to send measurements to a distant cloud or scattered nodes in the fog. Also included is a decentralized storage system that collects, processes, and saves the acquired information to share accurate, trusted, and cyber-secure information with medical scientists, clinicians, and caregivers.

GlucoCoin was created as an incentive scheme for individuals to provide fresh information to the system, as well as digital money. Using a blockchain capable of executing smart contracts, this system may automate CGM sensor purchases or compensate users who provide their information to enable the system function.

Muthanna et al.[9] proposed a framework for software-defined networking (SDN) to regulate and manage an edge computation layer of fog nodes and provide great availability and dependability for delayed IoT applications. OpenFlow switches with resource constraints are used in the SDN network, which has dispersed controllers. Trustworthy decentralization may be achieved with the usage of the blockchain. OpenFlow switches will be assigned computational processing duties depending on their present workload through an information-offloading technique. A traffic model has been suggested for the network as a whole. The algorithm is tested using simulation and a testbed.

Srivastava et al.[10] discussed FC, blockchain, and the IoT in healthcare. Unlike cloud computing, which operates among cloud and end-user devices known as IoT appliances, FC extends cloud computing's capacity to execute functions such as processing, saving, and interaction across the Internet. It offers superior information storage facilities with real-time access, reduced delay, greater responsiveness, better fault tolerance, and a protected and concealed context. Fog, access, information interface, application, and protection layers are all fragmented into five levels in the IoT system. The authors highlighted blockchain technology and consensus mechanisms to improve information protection in the healthcare context.

Yánez et al.[11] suggested a new context-aware approach for on-chain information allocation in IoT-blockchain networks. Additionally, they create a data controller using fuzzy logic, which estimates a request's RoA value using several context characteristics, such as the quality and quantity of the information and the networks it is being sent over. The mechanism's design and implementation also led to the refining of two popular IoT-blockchain architectural features. The data allocation method is instantiated in the blockchain-dependent cloud and fog architectures and evaluated using Fog Bus to show the efficacy of our approach. Using real-world healthcare uses, they also compare our method to current decision-making processes.

Kumari et al.[12] provided an examination of the functions of fog and cloud computing and the IoT in providing continuous context-aware services to end users when and where they are needed. For real-time information gathering, processing, and transfer, they suggest a three-layer patient-driven healthcare framework. It provides end users with information on the usage of fog devices and gateway in the Healthcare 4.0 ecosystem for present and future uses.

Pareek et al.[13] mentioned that the IoT links many gadgets throughout the globe. To relieve the strain on healthcare systems, IoT-dependent technologies may help decrease healthcare expenses, as well as boost computing and speed of processing. In the IoT, greater and more sophisticated healthcare information sets need the use of cloud computing. Delay, bandwidth usage, real-time reaction latency, security, and confidentiality are just a few of the problems that come with integrating IoT with the cloud. When it comes to cloud computing, many concerns and challenges must be addressed before any of the IoT-Fog-based system model designs can be evaluated.

Hanumantharaju et al.,[14] mentioned that the role of the IoT might help patients and healthcare providers keep in touch and offer their community clear, value-dependent care by making it simpler for both to remain in contact. FC may serve as the foundation for using IoT in healthcare. The experts discussed healthcare 4.0. Researchers will explore how FC taxonomy might be the best answer to healthcare 4.0 in terms of information gathering and evaluation, protection and confidentiality, and e-healthcare services.

Mayer et al.[15] proposed a FC architectural paradigm that integrates blockchain, FC, and the IoT for the healthcare area. For the most part, the FC architecture and its differential approaches to overcoming IoT restrictions are the most significant contributions.

The related literature review suggests that integration of fog architecture with blockchain utilizing capabilities of IoT devices is an interesting domain if we can incorporate a suitable algorithm for proper working.

This article proposes a FB-ECC algorithm for data encryption, with optimization accomplished by the GBCOA. This algorithm is compared with various algorithms proposed in different articles for its performance analysis.

Proposed Method

An effective blockchain-dependent protected healthcare service in FC is explained briefly in this section. The fog node gathers the information from the medical sensor devices and the data are validated using smart contracts in the blockchain network. To encrypt the data, the FB-ECC algorithm is proposed. To optimize the encryption process, the GBCOA is implemented. The performance of the suggested methodology is assessed and compared with the traditional approach. Figure 2 shows the flow illustration of the implemented techniques.

Four levels may be detected in this infrastructure: the IoT layer, the fog with blockchain layer, the cloud layer, and the data analysis layer. Patients' health information is acquired utilizing medical sensor devices. With wired or wireless accessible media, including ZigBee and Wi-Fi, every IoT medical equipment may be linked to a single Fog node. Fog nodes impose preset protection standards to control connected IoT devices and services, as well as serve as an intermediary between the Cloud and the Blockchain, allowing authorization index for information queries.

Data Validation Using Smart Contract

Although the word was used previously in the context of protocols among strangers on the internet, smart contracts are examples of contracts implemented on the Ethereum blockchain. A smart contract has the following rules:

1. Negotiate the agreement's conditions
2. Validate the agreement automatically
3. Implement the agreed conditions

A smart contract is made up of many functionalities that may be accessed from outside of the blockchain or through other smart contracts. The use of blockchain in conjunction with smart contract technology eliminates the need for transactional parties to rely on a centralized system. Every linked participant in the network has a replica of the smart contracts since they are kept on the blockchain. When initiated by an allowed or agreed-upon event, a smart contract may perform the agreed-upon stored procedure. Every contract transfer, as well as the whole audit trail of activities, are saved in chronological order for future access. Any party attempting to alter a contract or transaction on the blockchain will be detected and prevented by all other participants. The system continues to work even if one of the parties crashes, with no loss of information or integrity. As a result, a huge, safe, logical computer system is created without the dangers, expenses, or trust difficulties associated with a centralized paradigm.

Block Verification Using Stellar Consensus Protocols

The Stellar Consensus Protocol is a decentralized consensus protocol in which nodes in a network do not have

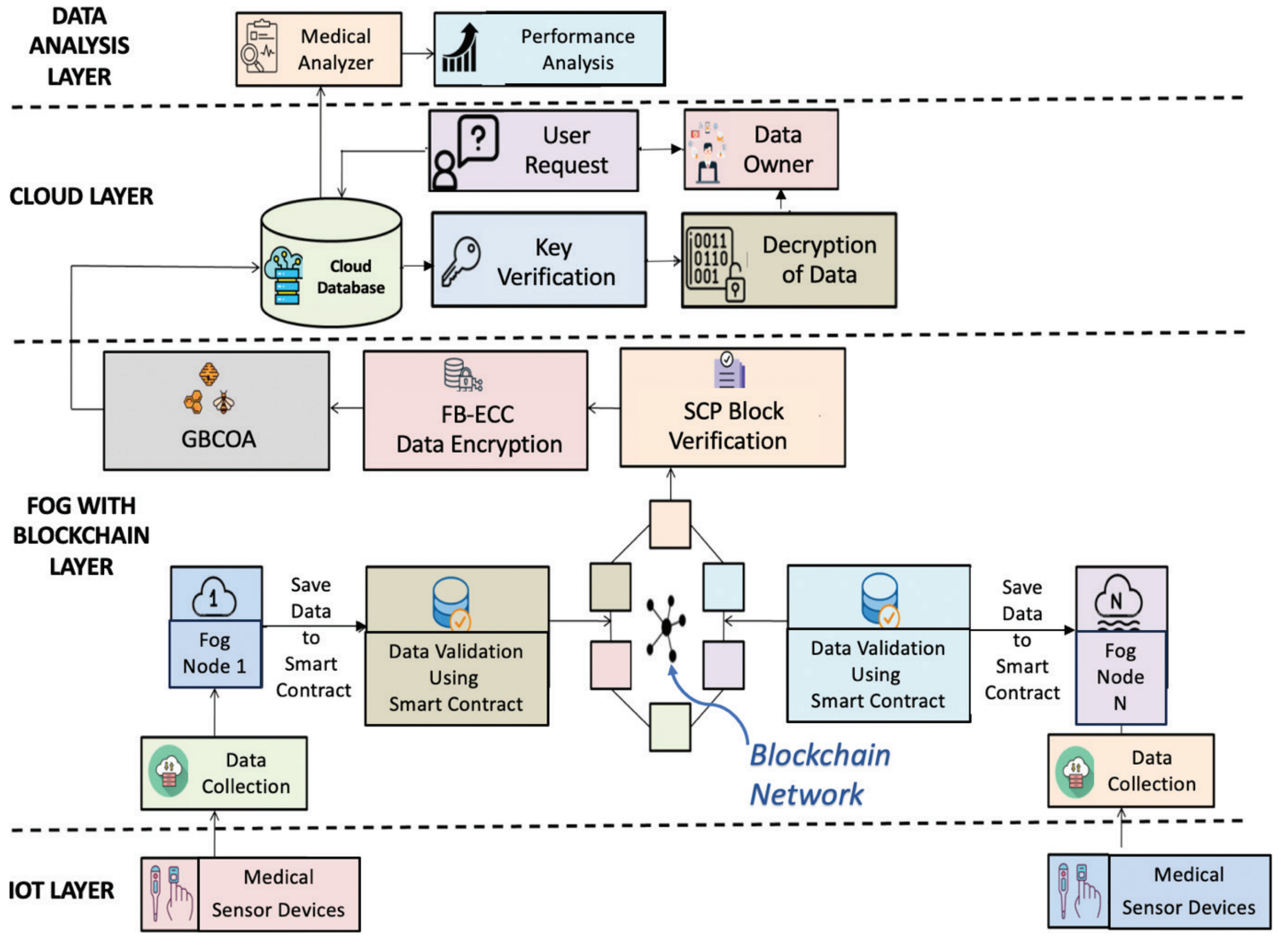

Fig. 2. Flow illustration of the implemented techniques. FB-EEC: functionally biased elliptic curve cryptograph; FC-BC: fog computing-block chain; GBCOA: galactic bee colony optimization algorithm, IoT: Internet of Things.

trustworthiness in all nodes in the network and may instead pick which nodes they trust.[16] The idea of a "quorum slice," which was initially established by this protocol, refers to a collection of nodes that trust one another. A "quorum" is a group of nodes large enough to establish a consensus, while a "quorum slice" is a subset of a quorum that persuades one or more nodes to agree.

Every node that gets these values will check the block for a single value among them, resulting in a single value being used to validate the block. Nodes begin checking the block on whether or not to accept or abort the values chosen in the prior stage throughout this stage. If a group of nodes cannot agree, the value is transferred to a greater block for authentication.

Data Encryption Using Functional Biased Elliptic Curve Cryptography Algorithm

The FB-ECC is a well-known public key cryptography technology that reliably and safely keeps the confidentiality and secret of encoded medical information. Identical keys are used for encryption and decryption (Table 2).

The FB-ECC is a common public key encryption method that uses distinct key pairs for encryption and decryption procedures, such as the randomized creation of public and private keys. Public-key cryptography techniques, such as FB-ECC, are also integrated into this technology. Authorization and clarity of new transactions depend on the dispersed agreement (greater than 50%) between its users, which gives this technique an edge over public-key cryptography. Because only the FB-ECC secret key can return the actual information, the medical information that is concealed cannot be retrieved by any unauthorized individual.

In asymmetric key cryptography, the FB-ECC technique plays a crucial role in conducting public key cryptography. Furthermore, a numerical expression is created utilizing the defined base point, curve, and the highest limit of a prime number function, and encryption is done by using the following FB-ECC equation:

$$k^2 = l^3 + bl + c \tag{1}$$

Table 2. A functional biased elliptic curve cryptography algorithm

```
Input: Input data (dI), private key (K).
Output: Encrypted data (Ed).
1: Randomly generate the public key (Pk);
2: $P_k = A * G_o$/* the function of generation Go depending on the curve equation, Go is extracted from the mapping function.
3: Generate the ciphers Cs as Cs ← RM * Go;
4:The encrypted data $(E_d)$ is created as $E_d \leftarrow (S_M * Pa) + (d_p, W);$/* W /* W denotes the base point on the curve.
5:The encrypted data ($E_d$) is uploaded to the public cloud environment
```

Note: See text for greater context.

The integers are indicated by the *b* and *c*. However, the encryption process's overall strength is determined by the production of a key depending on every cryptographic algorithm. The initial process is to make the public key that will be used to encrypt the information, which is usually received from the receiver. The second process is to generate a private key, enabling decryption of the original information on the recipient's side. *W* is the curve's starting point, and *A* is the chosen random integer within the range of 1– (m – 1):

$$S = A \, x \, W \qquad (2)$$

The public key is represented as *S*, whereas the private key is signified as *A*.

Encryption is a method of transforming actual information into ciphertext information, and it is used to increase protection. The FB-ECC is the most often used technique in cloud security to provide protection depending on the complexities of issues. The encryption procedure's strength is determined by the key generation process, which may give a better solution for information by supporting more confidentiality in the transmission of secret keys between various communication entities. The input original information dI and the private key K are supplied as inputs in this encryption procedure, and the generating function (Go) creates the public key (Pk). As a consequence, the cipher Cs are created using the 4-bit random numbers Rm and Go. The input data dI is then encoded using the curve's base point *W*, followed by the generation of the public key Pk and the random number Rm.

Galactic Bee Colony Optimization Algorithm

The GBCOA simulates the motion of stars, galaxies, and super galaxies to find feasible alternatives in a given search space. Like stars in galaxies, communicate with one another. The agent is divided into two levels by the galactic bee colony. The stars are shown on the first level, while galaxies are represented on the second level. Except for the starting population of the second level, which is drawn from the best solutions of the first level, every level has its search mechanism. At every stage, several search techniques may be used. In all stages, the researchers opted to employ the bee colony optimization method. So, at the first level, every subpopulation uses BCO to find the optimal answer, and then sends it to the higher level to build super bees. Super bees are utilized as the starting population in a new BCO run to find the optimum solution. The BCOA multilayered strike is represented in (3):

$$s_q^p \in S_p : q = 1, 2, \ldots, M$$

$$b_p \in S_p : b_p = best\left(S_p\right)$$

$$G = \bigcup_{p=1}^{M} b_p \qquad (3)$$

The first subpopulation of N solutions is generated randomly in the original galactic bee optimization technique. S_q^p denotes the jth solution of the ith subpopulation. S_p denotes the ith subpopulation. b_p (best(S_p)) indicates the great solution of the subpopulation S_p. Set G denotes superpopulation that comprises of the best solutions comes from subpopulations.

The better solutions gotten from each subpopulation in stage 1 are used as the first population of stage 2. Stage 2 is run L2 times then great outcome identified in stage 2 agreed as the last solution of the epoch. The total algorithm is run epoch count times then great outcomes identified so far in epochs agreed as the last outcome of the algorithm.

Cloud Database

A centralized health record server communicates with a medical record repository or database under this paradigm. The patient owns the information, which includes sensitive personal information. The patient's medical record, which is often contained in such documents, may also include biometric data, physical, psychological and mental health issues, personal history, allergies, medicines used, medical conditions, prior medical therapies, and illnesses, among other things. Financial data, including bank account, credit and debit card numbers, as well as the patient's identity, may be included in the medical records.[17]

The protection of the security and confidentiality of electronic health records is regarded as a core element of health information management. The major goal of the health data system is to guarantee that information is accessible when it is required and that it is not improperly utilized, disclosed, acquired, changed, or destroyed while being saved or sent.

The Security Privacy Standards work together to ensure suitable controls and safeguards. The patient identification number is used to identify the medical record in the medical record store or database. Under the IDs stated, the patient's healthcare information is personally identifiable. The patient's data might be utilized alone or in conjunction with additional data. The patient information is stored in databases on the virtual computer in the private cloud.

For information management, the private cloud architecture includes computation, storage, and network services. While delivering health information to the cloud, the encryption and hash operations are done according to the private cloud security framework. The actual health record information is kept in one database, while the key necessary for encryption is saved in another. As a result, an attacker's access to critical patient information stored in the cloud electronic health record database is restricted. As a result, the suggested framework safeguards the patient's sensitive data by ensuring information confidentiality and integrity. As a consequence, healthcare users may decrypt data and access crucial information from anywhere and at any duration.

Performance Analysis

The proposed model's performance assessment criteria for safe storage of encrypted medical information in a FC framework employing blockchain and a functional biased ECC algorithm are described. The key generation time (KGT), encryption time (ET), decryption time (DT), and level of security are used to assess the protected storage section of this suggested algorithm system. Moreover, the relevant formulae for estimating the various time are given in Equations (4), (5), and (6).

Encryption Time

The encryption time is described as the time taken to encrypt the information in milliseconds. It is calculated as follow:

Encryption time = End time – Starting time

$$KGT = ITT + ET \tag{4}$$

Where ITT represents the Information Transferring Time, while ET stands for Encryption Time. The ET computed here is the time it took the information to encode the original information and transform it to encrypted information. Where ENDT denotes the end time and STARTT indicates the starting duration of the encryption procedure.

$$ET = ENDT - STARTT \tag{5}$$

Figure 3 displays the suggested technique's encryption time utilizing the functional biased ECC method. Researchers discovered that encryption time improved as the number of bits in the key became larger. Our suggested architecture, on the other hand, takes much less time to encrypt than traditional approaches like Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA).

Decryption Time

The time necessary to decode the encrypted information is referred to as decryption time, and it is calculated as follows:

Decryption time = End time – Starting time

Here, the DT (decryption time) is computed as the amount of duration it takes the information used to decode the encrypted information in milliseconds, and it is calculated using Equation (6).

$$DT = ENDT - STARTT \tag{6}$$

Figure 4 depicts the suggested framework's decryption times versus traditional ways Decryption duration raises with increasing key size due to the introduction of disruptive information in the cloud server and various

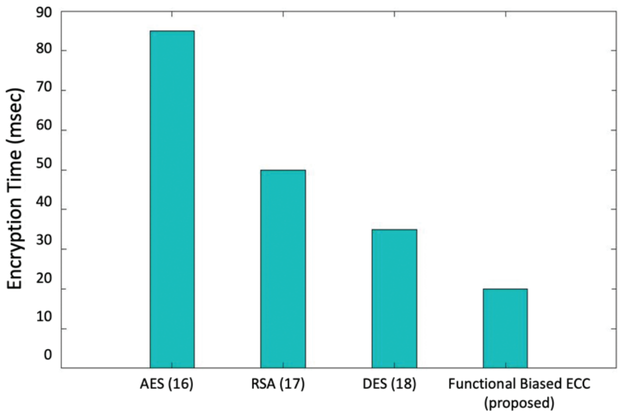

Fig. 3. Key generation time analysis. AES: Advanced Encryption Standard, DES: Data Encryption Standard, ECC: elliptic curve cryptography, RSA: Rivest-Shamir-Adleman.

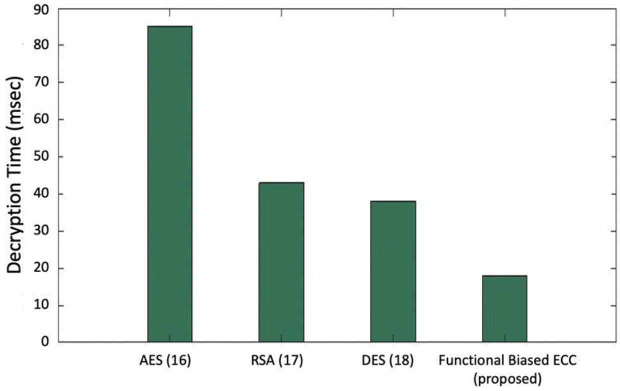

Fig. 4. Decryption time analysis. AES: Advanced Encryption Standard, DES: Data Encryption Standard, ECC: elliptic curve cryptography, RSA: Rivest-Shamir-Adleman.

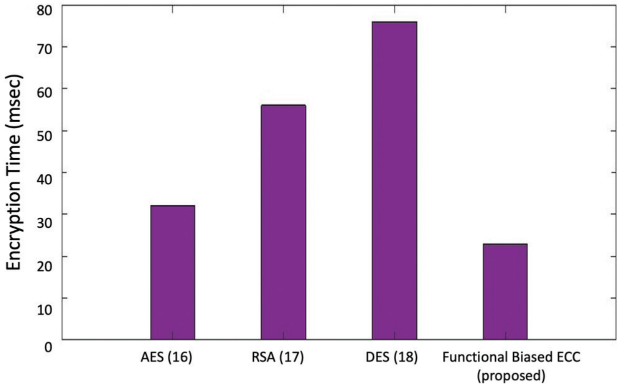

Fig. 5. Key generation time analysis. AES: Advanced Encryption Standard, DES: Data Encryption Standard, ECC: elliptic curve cryptography, RSA: Rivest-Shamir-Adleman.

keywords. When compared to traditional approaches such as AES, DES, and RSA, it has been shown that our suggested methodology takes less duration to decode even with larger keys.

Key Generation Time

From Figure 5 it can be observed that compared to traditional approaches such as AES, DES, and RSA, the suggested secured storage functional biased elliptic curve encryption algorithm consumes less time.

Security Level

Figure 6 compares the proposed functional biassed ECC to conventional secure storage algorithms like DES, RSA, and AES in terms of security level. In comparison to traditional methodologies, the presented alternatives offer a higher degree of security.

Figures 3 to 6 illustrate the comparisons between various algorithms such as AES, RSA, DES with proposed method FB ECC on various parameters such as:

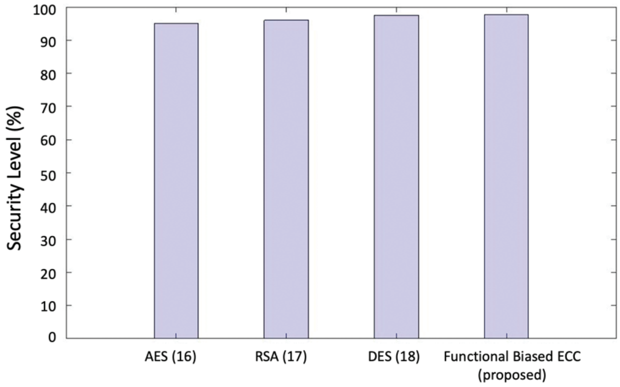

Fig. 6. Security level analysis. AES: Advanced Encryption Standard, DES: Data Encryption Standard, ECC: elliptic curve cryptography, RSA: Rivest-Shamir-Adleman.

i) Encryption time
ii) Decryption time
iii) Key generation time
iv) Security level

The overall analysis of algorithms shows that it gives much better results than traditional algorithms on all of the four discussed parameters.

Conclusion

To protectively store patient medical information in fog-enabled cloud databases, a secure medical information storage model is designed and included in this system. Medical information is gathered from numerous patients who support the e-healthcare gadgets in this system.

The FB-ECC technique is used to deploy a private server that requires decryption and encryption for computing. The functionally FB-ECC method is used in this research to execute the encryption, decryption, and key generation procedures on protected storage architecture. When compared to existing approaches, the suggested techniques outperform them in terms of security, encryption, decryption, and KGT. The suggested encryption algorithm, FB-ECC, has a security level of 98.64%. It has been shown that combining FC with blockchain has improved the security of information transfer in healthcare. Because only the functionally biased ECC secret key can return the actual information, the medical information that is concealed cannot be retrieved by any unauthorized individual.

Future studies in this area might include the development of a new cryptographic algorithm, which is an upgraded-level suggested encryption approach of FB-ECC with a higher degree of security.[18]

Funding

No funding was used in the preparation of this article.

Conflicts of Interest

There are no conflicts of interest.

Contributors

The authors are responsible for development of this article.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

Data are not available.

Application of AI-Generated Text or Related Technology

These was no use of AI.

References

1. Bouachir O, Aloqaily M, Tseng L, Boukerche A. Blockchain and fog computing for cyberphysical systems: the case of smart industry. Computer. 2020 Sep;53(9):36–45. https://doi.org/10.1109/MC.2020.2996212
2. Eskandarian A. Scanning the issue. IEEE Trans Intell Transp Syst. 2023 Sep 1;24(9):8899–918. https://doi.org/10.1109/TITS.2023.3299370
3. Onasanya A, Elshakankiri M. Smart integrated IoT healthcare system for cancer care. Wireless Netw. 2021;27:4297–312. https://doi.org/10.1007/s11276-018-01932-1
4. Ngabo D, 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. 2021 Aug 30;10(17):2110. https://doi.org/10.3390/electronics10172110
5. Baniata H, Kertesz A. A survey on blockchain-fog integration approaches. IEEE Access. 2020 Jun 1;8:102657–68. https://doi.org/10.1109/ACCESS.2020.2999213
6. Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, et al. The security of big data in fog-enabled IoT applications including blockchain: a survey. Sensors. 2019 Apr 14;19(8):1788. https://doi.org/10.3390/s19081788
7. Banerjee A, Mohanta BK, Panda SS, Jena D, Sobhanayak S. A secure IoT-fog enabled smart decision making system using machine learning for intensive care unit. In: 2020 International Conference on Artificial Intelligence and Signal Processing (AISP). 2020 Jan 10 (pp. 1–6). IEEE [cited 2024 Aug 05]. Available from: https://www.researchgate.net/publication/340896382_A_Secure_IoT-Fog_Enabled_Smart_Decision_Making_system_using_Machine_Learning_for_Intensive_Care_unit.
8. Fernández-Caramés TM, Froiz-Míguez I, Blanco-Novoa O, Fraga-Lamas P. Enabling the internet of mobile crowdsourcing health things: a mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. Sensors. 2019 Jul 28;19(15):3319. https://doi.org/10.3390/s19153319
9. Muthanna A, Ateya A, Khakimov A, Gudkova I, Abuarqoub A, Samouylov K, et al. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. J Sensor Actuator Netw. 2019 Feb 18;8(1):15. https://doi.org/10.3390/jsan8010015
10. Srivastava A, Jain P, Hazela B, Asthana P, Rizvi SW. Application of fog computing, Internet of Things, and blockchain technology in healthcare industry. In: Fog Computing for Healthcare 4.0 Environments: Technical, Societal, and Future Implications. 2021:563–91. https://doi.org/10.1007/978-3-030-46197-3_22
11. Yánez W, Mahmud R, Bahsoon R, Zhang Y, Buyya R. Data allocation mechanism for Internet-of-Things systems with blockchain. IEEE Internet Things J. 2020 Feb 10;7(4):3509–22. https://doi.org/10.1109/JIOT.2020.2972776
12. Kumari A, Tanwar S, Tyagi S, Kumar N. Fog computing for Healthcare 4.0 environment: opportunities and challenges. Comput Elect Eng. 2018 Nov 1;72:1–3. https://doi.org/10.1016/j.compeleceng.2018.08.015
13. Pareek K, Tiwari PK, Bhatnagar V. Fog computing in healthcare: a review. In IOP Conference Series: Materials Science and Engineering 2021 Mar 1 (Vol. 1099, No. 1, p. 012025). IOP Publishing.
14. Hanumantharaju R, Pradeep Kumar D, Sowmya BJ, Siddesh GM, Shreenath KN, Srinivasa KG. Enabling technologies for fog computing in healthcare 4.0: challenges and future implications. In: Fog Computing for Healthcare 4.0 Environments: Technical, Societal, and Future Implications. 2021:157–76.
15. Mayer AH, Rodrigues VF, da Costa CA, da Rosa Righi R, Roehrs A, Antunes RS. Fogchain: a fog computing architecture integrating blockchain and internet of things for personal health records. IEEE Access. 2021 Sep 1;9:122723–37. https://doi.org/10.1109/ACCESS.2021.3109822
16. Munirathinam T, Ganapathy S, Kannan A. Cloud and IoT based privacy preserved e-Healthcare system using secured storage algorithm and deep learning. J Intell Fuzzy Syst. 2020 Jan 1;39(3):3011–23. https://doi.org/10.3233/JIFS-191490
17. Al Hamid HA, Rahman SM, Hossain MS, Almogren A, Alamri A. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access. 2017 Sep 28;5:22313–28. https://doi.org/10.1109/ACCESS.2017.2757844
18. Yadav K, Alharbi A, Jain A, Ramadan RA. An IoT based secure patient health monitoring system. Comput Mater Contin. 2022 Jan 1;70(2):3637–52. https://doi.org/10.32604/cmc.2022.020614