IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 February 2024, accepted 17 March 2024, date of publication 25 March 2024, date of current version 2 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3381528

RESEARCH ARTICLE

Elliptic Crypt With Secured Blockchain Assisted Federated Q-Learning Framework for Smart Healthcare

SUDHAKARAN GAJENDRAN[1], REVATHI MUTHUSAMY[2], KRITHIGA RAVI[2], OMKUMAR CHANDRAUMAKANTHAM[2], AND SUGUNA MARAPPAN[2]

[1]School of Electronics Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, Tamil Nadu 600127, India
[2]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, Tamil Nadu 600127, India

Corresponding author: Sudhakaran Gajendran (sudhakaran.g@vit.ac.in)

ABSTRACT In this paper, a novel Elliptic Crypt with Secured Blockchain-backed Federated Q-Learning Framework is proposed to offer an intelligent healthcare system that mitigates the attacks and data misused by malicious intruders. Initially, the entered IoMT data is collected from publicly available datasets and encrypted using the Extended Elliptic Curve Cryptography (E_ECurCrypt) technique for ensuring the security. This encrypted data is fed as an input to the blockchain-powered collaborative learning model. Here, the federated Q-learning model trains the inputs and analyzes the presented attacks to ensure better privacy protection. Afterwards, the data is securely stored in decentralized blockchain technology. Subsequently, an effective Delegated Proof of Stake (Del_PoS) consensus algorithm is used to validate the proposed framework. The experiment is conducted using the WUSTL-EHMS-2020 dataset and the performances are analyzed by evaluating multiple matrices and compared to other existing methods. The performance of the proposed framework can be assessed using multiple matrices and the results will be compared to other existing methods. As a result, the proposed method has achieved 99.23% accuracy, 98.42% precision, 98.12% recall, 98.27% F1 score, 59080.506 average throughput, 59080.506 average decryption time 1.94 seconds and an average encryption time of 1.84 seconds and are superior to conventional methods.

INDEX TERMS Ciphertexts, consensus mechanism, ECC method, end-devices, encryption and decryption, Markov decision process, Q-learning.

I. INTRODUCTION

Efficient healthcare systems are more important for a better quality of life worldwide. The traditional health care structure cannot evolve due to the rapid increase in the number of patients with chronic diseases. Traditional health care faces the challenge of ensuring continuous monitoring, both for patients and physicians. Due to the advancement of technology and computerization, greater impact is being made in the medical field through safe, fast and easier data analysis techniques. Machine learning (ML) techniques increase efficient data management and data analysis with high accuracy [1], [2]. ML and blockchain technologies are used in data analysis and ensure the security of medical data. With the help of blockchain technology, the confidentiality of medical data can be increased through transparent reporting, high security and minimal transaction costs [3].

With the advancement of the Internet of Things (IoT), patient activities can be easily monitored from anywhere using remote access devices over the Internet. The IoT also offers the possibility of rapid diagnosis and better treatment through continuous analysis and remote access to data [4]. IoT related technologies like Wireless Sensor Networks (WSN), Bluetooth, Li-Fi, Wi-Fi etc. are used in communicating, collecting, storing and sharing information over the internet. Blockchain with IoT provides a better, privacy-preserving and secure Smart Health System (SHS) [5]. In the COVID-19 pandemic, artificial intelligence (AI)

The associate editor coordinating the review of this manuscript and approving it for publication was Peter Langendoerfer.

and next-generation networking (NGN) enable intelligent and safe remote monitoring and control of patients. AI-powered NGN is based on blockchain, intelligence capabilities, communication, mobile edge computing and rapid response from health authorities [6].

Blockchain and Mobile Edge Computing (MEC) technologies are creating a new revolution in smart healthcare. It offers high security when storing Electronic Medical Records (EMRs). The MEC reduce healthcare cloud computing costs, increase quality of service (QoS) and provide high-speed computing services [7]. The IoT connection of medical devices (IoMT) ensures secure data transmission via third-party channels. ML techniques like Deep Neural Network (DNN) with blockchain identify intrusion and corrupted data in IoT devices during communication. Various attacks are detected and reported with the help of this IoMT [8]. A deep learning (DL) based secure blockchain-powered intelligent IoT technique is deployed to secure data transit, medical diagnosis and hash value encryption. This technique protects health data from attackers [9].

One of deep learning algorithms (DL) [10] such as convolution neural network based on Bayesian gray filter and blockchain is jointly used to develop diagnostic devices to improve accuracy and protect privacy in smart healthcare [11]. The performance of the DL model is increased by the amount of data trained by the model. In healthcare, there is no way to collect large amounts of health data due to data protection. To solve this problem, Federated Leaning (FL) is used in smart healthcare and FL uses a central aggregator server while still storing the patient data in the local database [12], [13]. FL solves the problem in SHS, e.g. to reduce the runtime of the system and to validate user data provided in the system itself. The use of FL increases the security of the secret transfer through user authentication [14], [15] in SHS. A secure hierarchical federated learning framework (SHFL) based on K-anonymity is built for the secure exchange of patient medical information. This K-anonymity is used to hide the location of the cluster devices [16]. Unevenly distributed data leads to training with low efficiency and lower accuracy. This problem can be reduced by using a privacy-preserving FL framework in fog computing [17], [18].

A. MOTIVATION

On the other hand, the inevitability to address significant issues comprising malicious attacks, data privacy, and service quality has drove the expansion of a Blockchain-Based Federated Learning Method in smart healthcare. The demand for innovative solutions that can expand the efficiency and security of healthcare systems is growing as due to the advancement of artificial intelligence and the emergence of worldwide epidemic events. This approach attempts to leverage the dispersed nature of MIoT devices and edge nodes by combining technologies such as blockchain and federated learning to provide a decentralized and robust framework for managing clinical data. But, the conventional federated learning approaches in the healthcare sector commonly depend on a central server to distribute and gather model parameters at the process of training. The centralized approach undergoes a notable risk as it becomes an attack-prone single point of failure. Moreover, there is an issue with confidentiality and data security if the sensitive medical data is not adequately protected by typical federated learning approaches. The integration of blockchain technology into federated learning offers a feasible way to address these limitations by facilitating complete decentralization and enlightening security, transparency, and immutability in information sharing across various healthcare entities. Thereby, the proposed method seeks to address the drawbacks of existing methods and construct a more privacy-preserving and secure framework for collaborative healthcare data analysis by fusing the concepts of federated learning with blockchain technology. The reliability and security of system are further improved by the usage of effective consensus protocols and enhanced encryption algorithms, which guarantee data security without compromising the integrity and accuracy of the models trained on distributed clinical data. Thus, the proposed work motivates to design a blockchain-powered federated learning model for smart healthcare.

The main contribution of the proposed work are,

- To introduce an Elliptic Crypt with Secured Blockchain assisted Federated Q-learning Framework for avoiding attacks in IoMT data.
- To propose an effective encryption scheme, Extended Elliptic Curve Cryptography (E_ECurCrypt) for securing the input data with higher integrity.
- To design a new learning model, the federated Q-learning for training the encrypted data and analyzing the attacks.
- To afford higher reliability, a decentralized blockchain mechanism is utilized and is validated through a robust consensus algorithm.
- To offer an effective Delegated Proof of Stake (Del_PoS) consensus algorithm for validating the blockchain technology.
- To validate the performance of the proposed work, different matrices are computed and perform comparison over other existing methods.

The rest of the organization is given by; section II represents the related works and problem statement, section III represents the proposed methodology, section IV represents the results and discussion, section V represents the conclusion and future scope.

II. RELATED WORKS

A lot of research has been done on storing and protecting private healthcare information which are explained below:

Tuli, et al. [19] developed the DL framework based on fog computing in the centralized IoT for the automatic diagnosis of heart diseases through efficient data processing with low latency. This framework automatically diagnose the heart

patient data. The DL model was used to calculate resources such as the Central Processing Unit (CPU) and the Graphical Processing Unit (GPU) for training and prediction. The HealthFog model was viewed and evaluated using various types of performance measurements, including accuracy, network bandwidth, power consumption, and response time. This framework enabled high accuracy and performance in diagnosing cardiac patient data. The limitation of this framework was that it required smarter group training to increase accuracy, but this framework used separate training nodes. Rahman et al. [20] developed the method to ensure privacy of Internet of Health Things (IoHT) using FL and blockchain techniques like DP. This method used the fully encrypted dataset and model training. To aggregate the efficient model parameters, each federated edge node performs additive encryption while the blockchain operates with multiplicative encryption. The IoHT-based system proves to be a strong and efficient method in health management compared to other DL methods. The limitation of this method was that the Trusted Execution Environment (TEE) caused the difficulty in computing GPU memory for cloud providers.

Deep federated q-learning (DFQL)-based network slicing was described by Seifeddine Messaoud et al. [21] for Industrial IoT (IIoT). In order to enable differentiated QoS services in future IIoT networks, this method aimed to provide a federated and dynamic network management and resource allocation. To meet the QoS requirements of the IIoT slices, spreading factor (SF) and transmission power (TP) must be allocated. There were two primary phases to influence the DFQL. In the first phase, a multi-agent deep Q-learning dynamic slices approach was used to optimize self-QoS requirements concerning both delay and throughput. In the next phase, by applying the shared experiences of agents, deep federated learning was used to learn multi-agent self-models and permit to determine the best action that would fulfill IIoT virtual network slice QoS reward. In contrast to conventional methods, simulation results of DFQL framework had demonstrated an efficient performance. However, the complexity was higher. For the secure transmission of medical patient data, Al-Marridi et al. [22] proposed a solution based on deep reinforcement learning (DRL) and blockchain. This low-cost blockchain technology has intelligently and automatically changed the structure while increasing security and reducing latency. This model was created as a Markov Decision Process (MDP) that includes three RL techniques such as Dueling Double Deep Q-Networks (D3QN). Deep Q-Networks (DQN) and Double Deep Q-Networks (DDQN) have been used to effectively solve MDP. The Healthcare RL method is evaluated using the Random Selection (RS) method and offers high performance compared to other methods such as DQN, DDQN and D3QN. However, the RS method resulted in poor performance on average accumulated rewards.

Ali, et al. [23] proposed the method to solve the privacy issues in FL and blockchain-based IoT health applications. FL based privacy issues were solved using the central Orchestrator server and was useful to learn the process without updating the sensitivity data on the central server. FL used the model parameters for learning process and thus ensured high confidentiality of the patient data. Blockchain privacy issues have been solved using Differential Privacy (DP). Here, noise was added to the original data to protect the medical data with less processing power. Implementing this method, blockchain-based IoT devices improved privacy and security. When there were multiple queries, the balance between privacy and accuracy rate tends to be complex. Poap et al. [24] proposed an architecture to ensure patient medical data privacy through the Internet of Medical Things (IoMT) based on a multi-agent system. The multi-agent system divides the process into agents. This multi-agent idea was used to perform parallel classification training and achieve a single classifier architecture by grouping the classifier weights. Using the blockchain multi-agent system, the patient data was securely shared and protected during the transmission of medical data. The limitation of this model was the high delay in data transfer.

Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system was suggested by P. Chinnasamy et al. [25]. Here, a reliable smart contract-based access control system was utilized and enhanced the security when exchanging electronic health records between different patients and medical professionals. This was a proactive approach for safe data sharing in mobile computing while shielding private medical records from attacks. The framework valuation and protection technique was assessed by noting improvements in the viability of lightweight access control architecture, low network expectancy, and significant degrees of data concealment and security. Suyel Namasudra and Sagnik Datta [26] presented a smart contract model based on blockchain that uses consumer electronics and mobile edge computing to secure healthcare transactions. It safeguards the system throughout the patient-doctor Health Information Exchange (HIE) process. Here, EMRs and diagnosis reports are generated and uploaded using consumer electronics devices and MEC. The proposed scheme stores EMRs securely so they cannot be tampered with and are always accessible to authorized users. It does this by using techniques such as Advanced Encryption Standard (AES), Rivest Shamir and Adleman (RSA), Edwards-curve Digital Signature Algorithm (EdDSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and Inter-Planetary File System (IPFS). However, the encryption time and decryption time was higher.

Currently, various techniques to solve the security problems in smart health systems have been developed. Due to their limited abilities, they failed to achieve better results. Several studies used different encryption schemes to ensure data integrity and privacy, but security is also the primary concern. This investigation's focus is on the challenges that arise in the field of smart healthcare, explicitly with regard to protecting sensitive data, preventing harmful assaults, and guaranteeing excellent service quality. The necessity for

TABLE 1. Contribution and limitations of the existing methods.

Author	Method	Contribution	Result	Limitation
Tuli, et al. [19]	DL framework based on fog computing	To offer automatic diagnosis of heart diseases through efficient data processing with low latency	Better accuracy, network bandwidth, power consumption, and response time	Needed smarter group training to increase accuracy.
Rahman et al. [20]	FL and blockchain	To ensure privacy of IoHT using an efficient and strong mechanism	Improved security performance	Difficulty in computing GPU memory, need to minimize encryption and decryption time.
Messaoud et al. [21]	DFQL	To provide a federated and dynamic network management and resource allocation for meet the QoS requirements	Efficient performance in terms of different evaluation metrics	More complexity.
Al-Marridi et al. [22]	DRL	To secure transmission of medical patient data by integrating blockchain into deep learning	Improved the performance in terms of security	Need to improve performance on average accumulated rewards.
Ali, et al. [23]	FL and blockchain	To effectively solve the privacy issues in IoT health applications	Enhanced privacy and security	Need to improve accuracy.
Poap et al. [24]	Blockchain multi-agent consortium model	To guarantee patient medical data privacy through the IoMT based on a multi-agent system	Securely shared and protected data	High delay and less performance.
P. Chinnasamy et al. [25]	Smart contract-enabled secure sharing model	To offer a reliable smart contract-based access control system for enhancing the security	Viability, low network expectancy and better security	Need to minimize the complexity and improve the security performance.
Suyel Namasudra and Sagnik Datta [26]	Smart contract model based on blockchain	To secure healthcare transactions based on blockchain that uses consumer electronics and mobile edge computing	Enhanced the security parameters	Encryption time and decryption time was higher.

effective and secure healthcare solutions has increased due to the development of artificial intelligence and the occurrence of global health problems. Due to their frequent struggles with centralized data storage, the conventional healthcare systems are more susceptible to privacy violations and single points of failure. The incorporation of federated learning with blockchain technology offers a feasible solution to these challenges, expanding the efficiency and security of helath-care services. Thereby, the goal of the proposed method is to provide enhanced federated learning using blockchain technology in smart healthcare environments. At first, the ways that federated learning and blockchain technology can effectively use distributed clinical data to surge the accuracy of disease diagnosis as well as medical services is focused. Next, analyzed on how the proposed approach can ensure security and data privacy from different attacks by adversaries in the healthcare industry. Further, to avert attacks, preserve consensus, and thwart single points of failure, investigates on the effective mechanism. Through the investigation of these issues, the proposed method seeks to offer insights into the possible benefits and difficulties of incorporating blockchain-based federated learning in smart healthcare environments. Eventually intending to improve data security, patient privacy, and overall service quality in the healthcare industry.

III. METHODOLOGY

The development of artificial intelligence technology enables the smart healthcare system to offer more vital services. The openness and interconnectedness of smart

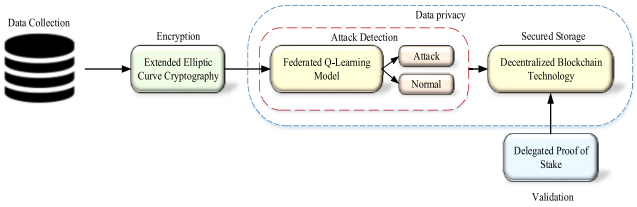

FIGURE 1. Basic block diagram of the proposed model.

healthcare facilities, however, make them vulnerable to attack and misuse by malicious outsiders, which emphasizes the importance of cyber security. Therefore, the suggested study created a unique elliptic crypt with Secured Blockchain aided Federated Q-learning Framework to address this issue. Data collection, encryption, attack detection, safe storage, and validation are all part of the proposed system. IoMT input data are initially gathered from publically accessible datasets. The Extended Elliptic Curve Cryptography (E_ECurCypt) method is used to encrypt the inputs in order to ensure their security. Input for the proposed block chain-assisted federated learning model is provided via these encrypted data. As a result, a greater level of privacy protection is provided by the federated Q-learning model, which trained the inputs and examined the assaults that were given. Finally, using decentralized blockchain technology, the data are safely kept. The proposed system is validated using the Delegated Proof of Stake (Del_PoS) consensus mechanism. Several matrices are evaluated in order to assess the effectiveness of the proposed structure and results are then contrasted with those obtained using other existing methods. Figure 1 represents the basic block diagram of the proposed model.

A. EXTENDED ELLIPTIC CURVE CRYPTOGRAPHY

Encryption data produced by the IoMT is vital in healthcare since it helps to protect private and sensitive patient data from breaches and unauthorized access. Robust encryption methods, comprising Secure Sockets Layer (SSL) and advanced encryption standard (AES), are employed to encrypt the data stored in IoMT devices and make the system indecipherable to outsiders. Through the use of sophisticated algorithms, the data is encoded during the encryption process, scrambling it into an unreadable format and only accessible to authorized users with required decryption keys. Healthcare organization can reduce the risks of data breaches and unauthorized access by implementing encryption in IoMT systems, protecting patient privacy and security. Thereby, encryption is indispensable to maintain the confidentiality and integrity of IoMT data, which encourages confidence in the increasingly associated healthcare delivery system. Elliptic curve cryptography (ECC) [27] is considered as a prominent encryption technique for protecting IoMT data in the healthcare industry because of its scalability, effectiveness, and strong security features. ECC offers comparable security with much smaller key sizes than standard encryption techniques such as RSA, and makes it more appropriate for IoMT devices with limited computational capacity and battery constraints. The IoMT networks transmit data in real time with less delay because of the faster encryption and decryption operations brought by reduced key size. Besides, the mathematical properties of ECC offer inherent resistance against emerging threats and guaranteeing the long-term sustainability and security of medical data. Furthermore, the smaller key sizes of ECC help to lower storage needs, which maximizes the use of storage resources in IoMT systems and devices. Overall, the use of ECC in IoMT contexts for healthcare not only reinforces security but also progresses performance and resource efficiency, building it an effective encryption technique for protecting sensitive patient data in an interconnected healthcare ecosystem.

In the proposed method, the IoMT data is encrypted using the Extended Elliptic Curve Cryptography (E_ECurCypt) encryption method. The introduction of E_ECurCypt serves as a more secure alternative against conventional ECC owing to certain the shortcomings and vulnerabilities. Standard ECC has several problems however, the major issue is the possibility of implementation flaws that compromise the encryption process's security. For encryption and decryption, standard ECC generally necessitates the creation of public and private keys, which cannot be enough to safeguard against sophisticated cyberattacks. On the other hand, E_ECurCypt alleviates these concerns by adding an additional secret key, which increases the complexity of the encryption scheme and strengthening its security against intrusions. E_ECurCypt is based on a curve with a defined base point computed from functions of primes as shown in Figure 2. Unlike E_ECurCypt, which generates a third key (secret key) to increase system security, Standard ECC only generates two types of keys: public and private. The decryption formula is calculated by subtracting the created secret key from it and adding it to the encryption formula. This increases the complexity of the two phases. It is quite difficult to identify the original data when both decryption and encryption are very complex processes. The security level of the data is increased immediately. Equations (1) to (7) are used to mathematically illustrate the extended ECC.

In the proposed method, the IoMT data is encrypted using the Extended Elliptic Curve Cryptography (E_ECurCypt) encryption method. The introduction of E_ECurCypt serves as a more secure alternative against conventional ECC owing to certain the shortcomings and vulnerabilities. Standard ECC has several problems however, the major issue is the possibility of implementation flaws that compromise the encryption process's security. For encryption and decryption, standard ECC generally necessitates the creation of public and private keys, which cannot be enough to safeguard against sophisticated cyberattacks. On the other hand, E_ECurCypt alleviates these concerns by adding an additional secret key, which increases the complexity of the encryption scheme and strengthening its security against intrusions. E_ECurCypt is based on a curve with a defined base point computed from functions of primes as shown in Figure 2. Unlike

E_ECurCypt, which generates a third key (secret key) to increase system security, Standard ECC only generates two types of keys: public and private. The decryption formula is calculated by subtracting the created secret key from it and adding it to the encryption formula. This increases the complexity of the two phases. It is quite difficult to identify the original data when both decryption and encryption are very complex processes. The security level of the data is increased immediately. Equations (1) to (7) are used to mathematically illustrate the extended ECC.

$$a^2 = b^3 + xb + y \tag{1}$$

Using integers x *and* y. The mechanism utilized to generate keys in a cryptographic operation influences the reliability of the encryption. The proposed approach requires the generation of three different types of keys. For the purpose of encrypting data, a public key is first created. Making a private key is the next step in the process of decrypting data. For data encryption, the public key is initially produced. A private key is subsequently produced and used to decode the data. Finally, a secret key is created using the private key, the public key, and the points on the elliptic curve. Assume that the elliptic curve's base point is at P_B. To create a private key Pv_k, pick a random integer among 0 and $i-1$. According to equations (2) and (3), the public key Pb_k is generated.

$$Pb_k = Pv_k * P_B \tag{2}$$

Evaluate the following equation:

$$Pb_k = \prod (Pv_k,\ P_B) \tag{3}$$

Equation (3) states that the secret key is created by adding Pb_k, Pv_k and P_B:

$$Sec_k = \sum (Pv_k,\ Pb_k,\ P_B) \tag{4}$$

Sec_k stands for the secret key. The values collected from the IoT devices are encrypted following the creation of the key. Two ciphertexts, equations (5) and (6) are contained in the encrypted data.

$$CT_1 = (Sec_1 * P_B) + Sec_k \tag{5}$$

$$CT_2 = m + (Sec_1 * Pb_k) + Sec_k \tag{6}$$

(6) If m denotes the original message, CT_1 and CT_2 stand for ciphertexts 1 and 2 and Sec_1 is a random integer that ranges from 1 and $i-1$, respectively. The decryption process yields the original data. Decryption is the opposite of encryption, therefore equation (7) shows that the secret key obtained during the decryption phase is removed from the standard equation for decryption.

$$m = ((CT_2 - Pv_k) * CT_1) - Sec_k \tag{7}$$

Input for the proposed block chain-assisted federated learning model is provided via these encrypted data. As a result, a greater level of privacy protection is provided by the federated Q-learning model, which trained the inputs and examined the attacks that were given.

B. ATTACK DETECTION BASED ON FEDERATED Q-LEARNING MODEL

Detecting and mitigating attacks through the incorporation of modern technologies like blockchain and federated learning has developed as a potential strategy in the healthcare industry, where patient data privacy and security are more significant. Sensitive medical data is initially encrypted as part of the process to ensure its security. In the proposed method, the encrypted data is fed to the input of new blockchain-assisted federated learning model, which combines the collaborative and privacy-preserving aspects of federated learning with the immutability of blockchain. In this system, the privacy of individual data sources is preserved by the federated Q-learning model, which is responsible for training on the encrypted inputs gathered from different healthcare entities. Through the application of reinforcement learning techniques like Q-learning, the model is able to incessantly progress its understanding of typical data patterns and distinguish deviations that can be a signs of anomalies or possible attacks. The model's ability to dynamically modify its detection abilities through adaptive learning reinforces its resilience to changing threats in the healthcare industry. Furthermore, the blockchain constituent is essential to uphold the transparency and integrity of the federated learning process. Blockchain technology preserves a decentralized, tamper-proof ledger of model updates and training data inputs from many participants, improving the system's overall auditability and reliability. Accordingly, federated learning with blockchain support enables increased privacy protection and efficiently identifies and counteracts attacks in the healthcare sector. This creative method provides healthcare organizations, the ability to protect patient information confidentiality and integrity while staying ahead of emerging attacks.

C. REINFORCEMENT LEARNING (RL)

According to its definition, reinforcement learning is a form of machine learning that incorporates agent interaction and improves reward accumulation for environmental activities. Dynamic programming techniques are used in machine learning's Markov Decision Process (MDP) to create the best possible strategy for maximizing rewards over time. Following are RL's crucial actions:

- To begin with, the agent interacts directly with surroundings in each of its states to conduct actions and gather data.
- Second, the environment responds to the activity made by granting as positive or negative rewards, respectively.
- Third, the agent optimizes the rewards already gathered by recognizing changes in the surrounding environment.
- Fourth, starting from the current situation, the RL approach will be used at this point to increase the predicted reward value.

Many confidentiality and secure systems, including intrusion detection and prevention systems (IDS) and intrusion detection systems (IPS), have incorporated RL as a component. It might be beneficial to employ a distributed RL

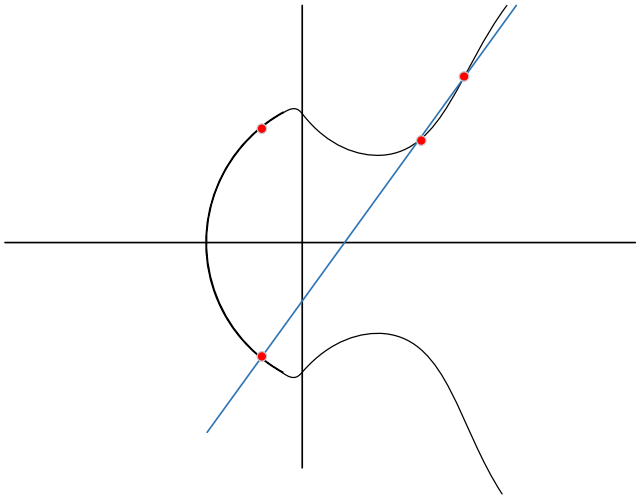

FIGURE 2. Elliptic curve.

process where every sensor/agent keeps track of the observations obtained from the states and sends them to a central sensor/agent. The agents at the top of the hierarchy are responsible for the analysis of the information collected and the transmission of the dangerous condition to the network moderator. The Markovian Reward Process (MRP) has been used to perform an RL-based IDS using a series of system calls to duplicate the behavior of system calls, transforming the intrusion detection to forecast the MRP value function. The research developed an adaptable neural network for IDS with the assistance of RL can identify new assaults on its own.

D. Q-LEARNING (QL)

A reinforcement learning method called QL uses the idea of value iteration, where the agent determines which action (N) yields the largest reward (R) by estimating the value function and updating all its states and behaviors for all iterations. It is not model-based and can deal with stochastic rewards in a non-adaptive way. In its most basic form, an agent in a state (S) performs an action (N), records its reward (R) along with the following state $\left(\hat{S}\right)$ and then predicts the Q value by applying equation (8), where N_i, R_i *and* S_i are the action, reward and state at time (i), $0 < \beta < 1$ is the learning rate and $0 < \chi < 1$ is the relative value of rewards, respectively.

$$Q^{+}\left(N_i,\ S_i\right) \leftarrow (1-\beta)\, Q^{+}\left(N_i,\ S_i\right) + \beta\left(R_i + \chi_{\max} Q^{+}\left(N_i^{+} S_i^{+}\right)\right) \tag{8}$$

"It is significant to note that this research picked Q-learning as one of the reinforcement learning techniques because of its model-free feature. Additionally, using Q-learning, stochastic incentives may be approached in a non-adaptive way. Furthermore, Q-learning is capable of learning without always following the rules at the moment. The future reward may be calculated using $K^{\lambda}(S)$ as described in equation (9), where $B_{SS^{+}}(N)$ denotes the probability of a state transition, $R\left(S,\ S^{+},\ N\right)$ denotes the reward calculated with the state transition and w is the weight of the reduction among the future and present rewards.

$$K^{\lambda}(S) = \sum_{N} \lambda(N, S) \sum_{S^{+}} B_{SS^{+}}(N)\, R\left(S, S^{+},\ N\right) + wK^{\lambda}\left(S^{+}\right) \tag{9}$$

In order to do this, the value iteration mechanism is calculated by the formula (10), where $K_j^{\lambda}\left(S^{+}\right)$ denotes the estimated value of R at S^{+} in its original iteration j and $K_{j+1}^{\lambda}\left(S^{+}\right)$ denotes the calculated value of R at the updated iteration $j+1$. It is important to keep in mind that each iteration can be completed with $G\left(|N|\,|S|^2\right)$ and that the amount of iterations in reinforcement learning can increase exponentially.

$$K_{j+1}^{\lambda}(S) = \max_{N} \sum_{S^{+}} B_{SS^{+}}(N)\, R\left(S, S^{+},\ N\right) + wK^{\lambda}\left(S^{+}\right) \tag{10}$$

Algorithm 1 FDL_{avg}

1: Technique: FDL_{avg} (End device side)
2: Receiver d_i from the central server
3: Initialize $d_{i,0}^{l} = d_i$ d_0: Server initialization
4: For $z = 0,\ 1,\ 2,\ \ldots$ do
5: Select a sample μ form F_{in} F_{in} = End device local dataset
6: Update $d_{i,z+1}^{l} = d_{i,z}^{l} - \left(d_{i,z}^{l},\ \mu\right)$
7: End for
8: Set $d_{i+1}^{l} = d_{i,Z_i}^{l}$
9: Send d_{i+1}^{l} back to the server
10: Technique FDL_{avg}(Central server)
11: Initialization: d_0: initialization of server model
12: For each iteration $i = 0,\ 1,\ 2,\ \ldots$do
13: $|T_i| = T \cdot L \geq 1$;
14: For each client $l \in |t_i|$ do d_{i+1}^{l} End device update
15: $d_{i+1} = \sum_{l \in t_i} \frac{x_l}{x_\beta} d_{i+1}^{l}\, x_\beta = \sum_{l \in t_i} x_l$
16: End for
17: End for

E. FEDERATED LEARNING (FDL)

Federated learning (FDL) represents a collaborative machine learning system [30] where data is gathered locally and taught at the enddevices. To create a global model, the training models are then averaged. End-devices only exchange the variables of their local models with the server and do not divulge the local training/testing datasets. Instead, they train their own models locally. The *FDL*-Averaging method (FDL_{avg}), which handles the end-device training models in the centralized server to produce a shared global method has been used in the proposed framework.

The Stochastic Gradient Decent (SGD) system [31] is used to execute reinforcement learning training on end devices by consideration of gradient descent optimization approximations and exchanging dataset variables with calculated values

after randomly selecting a subset from the primary dataset. FDL_{avg} takes into account three variables:

the percentage of end-device calculations, ii) the volume of mini-batch operations and iii) the number of training exercises performed on the end-devices dataset. On the end devices, these variables make it easier to share the gradient decrease. The server then averages the final trained models, offers a modification and transmits the updated models together with the updated variables for the subsequent round. The selected FDL_{avg} technique is briefly described in Algorithm 1.

Both the server system and the end devices are targeted by the FDL_{avg}. The server's global model, selected as d_0 is randomly adjusted to start. The first round then starts with the centralized server choosing a subset of the end devices (t_i such that $|t_i| = T$, $L \geq 1$) and dispersing its present global model d_i, among all of the end devices in t_i. When the server's shared model d_i is updated, the end devices update their own models (d_i^l). Then, the end devices divide their local datasets into size α-related subgroups and execute SGD Iterations. After receiving individual trained models from all end devices (d_{i+1}^l) and uploading them to it, the centralized server then builds the new updated global model d_{i+1} by performing a biased sum of all the aggregated local models as shown in Algorithm 1. The terms T, α, $iter$, ξ *and* σ denote the client's fraction, subset size (batches), iteration number prior to update the global model, learning rate and learning rate decay. For training reasons, SGD has adopted the acronyms ξ, α, *iter and* σ.

F. DECENTRALIZED BLOCKCHAIN TECHNOLOGY

To ensure the validity of the collected local data and learned models, blockchain is used to enable the federated learning process. Since decentralized tasks are usually based on the cooperation of untrustworthy end devices, a consensus mechanism must be taken into account to ensure that the tasks, data or services offered are correct and reliable. Blockchain technology is a decentralized [32], impenetrable ledger that builds trust without relying on a central authority. Blockchain is defined as a collection of blocks that, in its simplest form, keep the data for a collection of application-oriented transactions secret. Using hash pointers, the blocks are concatenated together using a cryptographic data model, with the header of each new block pointing to the hash of the previous block's contents. To confirm the order, content, and hash clues to the blockchain technology, participants verify the locally stored copies of the blockchain using a consensus process. Major IoT infrastructures can benefit from numerous valuable solutions that blockchain technology can offer, especially those that address trust and security concerns. For example, without using a central server, the blockchain can immediately provide a unique identity for IoT end devices. In addition, the endpoints use the unique identity and key to cryptographically sign the traffic routed from the endpoints to the blockchain. It enables secure and reliable exchange of device model updates by merging blockchain technology

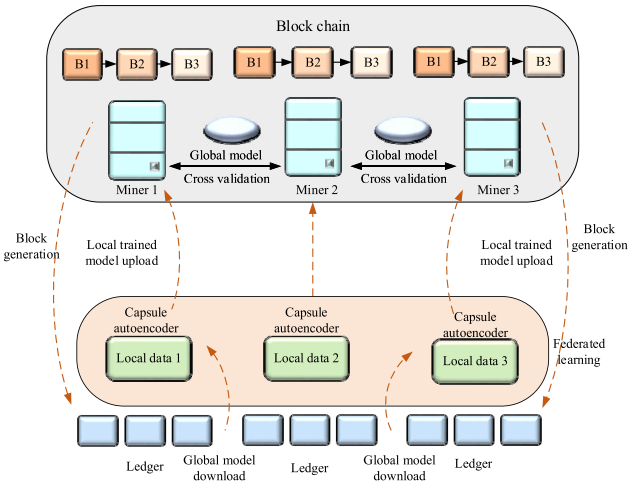

FIGURE 3. Updation procedure of proposed method.

with the crucial infrastructure provided by federated learning. Blockchain technology is used in the proposed strategy as an additional layer of defense to ensure device reliability. The blockchain is expanded to include the trusted devices, the untrusted devices are removed and not sent to the cloud. With the proposed blockchain-backed FL architecture, any consensus algorithm can be used. Nevertheless, the Del_PoS is extremely successful against defects, since end devices can be portable. The system is unaffected by terminals that fail to provide a consensus response or do so in an erroneous or erroneous manner, and consensus can be assured. Model validation is performed by miners, which can be trusted endpoints or edge devices.

The locally learned model is uploaded from each end device to the appropriate miner selected by the cloud. Miners perform mutual verification by exchanging updates to the local model and comparing it to the overall model. The local model changes are then checked using a consensus technique (i.e. Del_PoS) and a block is formed that keeps track of all updates. The block created is then included in the distributed ledgers, which are downloaded by the end devices to calculate the global model update. The blockchain-based model update process is shown in Figure 3. For example, the automobile can use Q-Learning to analyze its local data before sending the learned model to Miner 3, which then compares the trained local model to the global model and validates it using the consensus method. The latest changes are saved in a block and finally added as a record to the distributed ledger. The Del_PoS consensus algorithm is used to validate the proposed model.

G. VALIDATION USING DELEGATED PROOF OF STAKE (DEL_PoS) CONSENSUS ALGORITHM

Each blockchain contains unique techniques for establishing consensus about the inputs to be introduced into the network. Consensus layer, network layer, application layer, incentive layer, data layer and contract layer are the six layers that make

up the structure of the blockchain. The consensus mechanism is a cooperative algorithmic process that describes in detail how each consensus node comes to an agreement and how records are validated. Every blockchain user uses it to decide if the transaction is legitimate and to keep accounts in sync. As a result, each consensus node on the blockchain validates and evaluates the data using the algorithm. For a blockchain network the selection of consensus mechanism [33] is crucial since it has an instant influence on aspects like decentralization, scalability, security, and energy efficiency. The consensus mechanism Delegated Proof of Stake (Del_PoS) is unique among other consensus procedures such as Proof of Work (PoW), Proof of Stake (PoS), and practical Byzantine Fault Tolerance (pBFT) owing to various factors. At first, when comparing to PoW, DPoS provides a more scalable and energy-efficient alternative. In contrast to Proof of Work (PoW), which necessitates high processing capacity and energy consumption to solve intricate cryptographic puzzles, Del_PoS achieves consensus through a small group of elected delegates, significantly lowering the energy requirements and computational burden. In large-scale blockchain networks like those intended for smart healthcare, where data processing and real-time transactions are critical, this efficiency and scalability are more important.

Moreover, when related to conventional PoS and PoW algorithms, Del_PoS offers a greater degree of decentralization. Del_PoS distributes decision-making authority across a group of elected delegates selected by stakeholders while PoS can effect in centralization among the wealthiest participants as well as PoW lead to concentrate power among miners with the most computational resources. By promoting a more decentralized and democratic governance model, this strategy strengthens the network's resistance against centralization. In addition, Del_PoS has strong security features that are identical to pBFT. While Del_PoS accomplishes similar security through a reputation-based system, in which elected delegates are enthused to perform fairly to keep their reputation and rewards, pBFT delivers deterministic and quick finality by tolerating a specified amount of Byzantine faults. This guarantees byzantine fault tolerance while ensuring effective transaction finality and block production and makes Del_PoS as a compelling choice for applications that require both performance and security, like intellectual healthcare systems.

Del_PoS is an improved form of PoS with increased speed and high security features. The democratic nature of the blockchain is further defined by the fact that different users often vote on which delegation becomes the block producer. In the Del_PoS, a delegate is chosen to cast votes on behalf of other people who picked them and as a result, the Voters have the power. A new delegate may be elected in their place if the elected witnesses perform inadequately or inaccurately represent their constituents. The voters who choose the delegates receive a portion of the advantages they receive. The validation process is provided control by a small number of selected users. As they are in charge of verifying block chains and the structure allows users to choose who represents them, the delegates can misuse their position of power. The presence of such cartels renders the system vulnerable to assaults and lessens the decentralization of the blockchains.

TABLE 2. Hyper parameters.

Sl.No	Parameters	Values
1	Epoch	100
2	Batch size	32
3	Optimizer	Adam
4	Learning rate	0.001
5	Hidden size	100
6	Decay rate	0.99
7	Gamma	0.01
8	Epsilon	0.1

TABLE 3. Dataset details.

Measurement	Values
Size of dataset	4.4 MB
Number of normal samples	14,272
Number of attack samples	2,046
Total number of samples	16,318

IV. RESULTS AND DISCUSSION

The implementation is done by the PYTHON platform with the system specifications of Intel(R) Core (TM) i7-3770 CPU @ 3.40GHz with installed memory of 16 GB with an operating system of 64-bit without using a pen or touch input. The performance are evaluated based on the metrics of accuracy, precision, recall, f1-score and Area Under the Curve (AUC). Also, the recent baseline methods are chosen for comparing with proposed study. The existing models like Blockchain based XOR Elliptic Curve Cryptography (BC-XORECC) technique, DES, RC4, AES and Blowfish techniques are compared with proposed model. The hyper parameters are given in Table 1. The work is implemented using the WUSTL-EHMS-2020 dataset. The WUSTL-EHMS-2020 dataset's statistical data is shown in Table 2. This dataset contains 44 features including features for the label and network flow measurements.

Performance Matrices:

The proposed approach is evaluated by comparing it to current models in terms of accuracy, precision, recall and f1-score using a basic evaluation matrix such as true negative *TN*, true positive *TP*, false negative *FN* and false positive *FP*. More information about the assessment matrix is provided below:

- ➢ True Positive - The proportion of samples correctly classified as normal in the normal section and as a threat in the threat section.
- ➢ True Negative - The percentage of samples correctly classified as posing a threat to the normal portion or as posing a threat to the normal section.

- ➢ False positives are the number of samples that were wrongly recognized as threats in the threat section and as normal in the normal section.
- ➢ False Negative - The percentage of samples recognized mistakenly as normal in the threat and threat in the normal parts.

The performance of the proposed approach may be defined using the evaluation matrices as follows:

Accuracy- Accuracy is the percentage of samples that can be successfully located in the total data set. Because the data set is unbalanced, this statistic is irrelevant for comparing approaches. The accuracy may be expressed as follows:

$$Accuracy = \frac{TN + TP}{TN + TP + FP + FN} \tag{11}$$

Precision-Precision is the ratio of the number of samples properly recognized as normal in the normal section or as a threat in the threat portion to the total number of samples correctly identified as normal/threatening.

$$precision = \frac{TP}{TP + FP} \tag{12}$$

Recall-Recall is the proportion of samples correctly recognized as normal in the normal component or as a threat in the threat component relative to the total number of samples correctly categorized as normal/threat in the dataset.

$$recall = \frac{TP}{TP + FN} \tag{13}$$

F1-score- The harmonic mean of recall and precision is represented by the F1-score.

$$F1 - score = \frac{2 \times recall \times precision}{recall + precision} \tag{14}$$

Throughput-Throughput is the number of information units that a system can process in a given amount of time. It is frequently employed in devices ranging from organizations to various device components and networks. Through put can be expressed as:

$$Throughput \ \ (bits\,per\ \text{sec}) = \frac{Total\ packet\ received}{\text{time}} \tag{15}$$

A. PERFORMANCE EVALUATION

Figure 4 represents the confusion matrix of the proposed model. A confusion matrix deals with a binary classification procedure. The resultant table has two rows of data and two rows of columns which each containing four values: true positives, false positives, true negatives and false negatives. A real positive occurs in the confusion matrix when the result is positive and the prediction is positive. A false positive occurs when the result observed is negative while the prediction is positive. A real negative occurs when a result is negative with a negative predicted, while a false negative occurs when an assessment is positive with a negative prediction.

Figure 5 represents the performance of the proposed and existing model. The performance matrix such as accuracy, precision, recall and f1-score are used to evaluate the existing

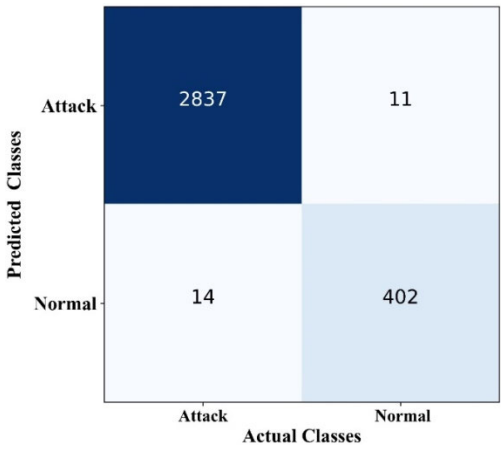

FIGURE 4. Confusion matrix.

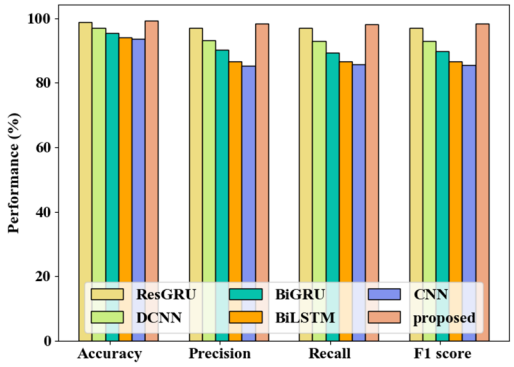

FIGURE 5. Performance analysis of proposed and existing model.

model and proposed approach. The existing model including ResNet, BiGRU, CNN, DCNN and BiLSTM are used which the ResNet achieved the value of 98.68% and BiGRU achieved the value of 95.49%. CNN have the accuracy value of 93.5% while DCNN and BiLSTM achieved the value of 96.9% and 94.02%, respectively. The precision value of the ResNet is 97.08% and the precision value of DCNN is 93.15%. The BiGRU, BiLSTm and CNN achieved the value of 90.28%, 86.59% and 85.31%, respectively. The recall value of the existing and proposed model is given as: ResNet have value of 96.98%, DCNN achieved the value of 92.88%, BiGRU have the value of 89.2%, BiLSTM have the value of 86.51% and CNN have the value of 85.6%, respectively. The F1-score of the proposed and existing model is given by: the ResNet have the value of 97.03%, the DCNN and CNN achieved the value of 93.02% and 85.45%, respectively. The BiGRU and BiLSTM have the value of 89.74% and 86.55%, respectively. The proposed model achieved the accuracy of 99.23%, precision value of 98.42%, recall value of 98.12% and F1-score of 98.27%, respectively. The figure states that the proposed model achieved the best performance among all other existing models.

Figure 6 represents the encryption time of the proposed and existing models. The data size is varied from 100 to 500 MB. The existing models like Blowfish, DES, RC4, AES and

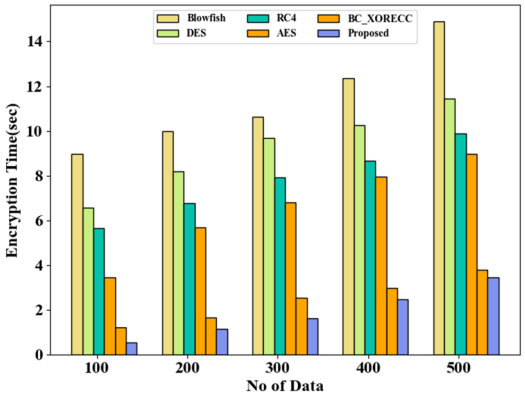

FIGURE 6. Encryption time vs data size.

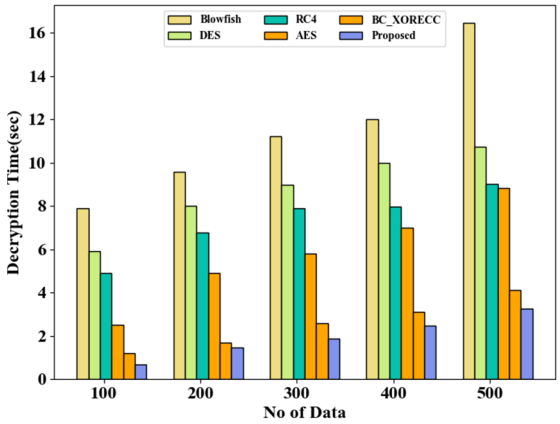

FIGURE 7. Decryption time vs data size.

BC-XORECC are used to evaluate the proposed model. The Blowfish algorithm achieved the value of 8.97 at 100 MB and achieved 14.89 at 500 MB while DES have the value of 6.55 at 100 MB and achieves the value of 11.45 at 500 MB, respectively. RC4 model achieved the value of 5.64 at 100 MB and 9.84 in 500 MB data size. AES model achieved 3.45 at 100 MB and later it becomes 8.97 when the data size becomes 500 MB. BC-XORECC model achieved the value of 1.2 when the data size become 100 MB and becomes 3.78 when the data size is 500 MB. The proposed model achieved the value of 0.54 when the data size is 100 MB and becomes 3.44 at 500 MB data size.

The figure 7 represents the decryption time of the proposed and existing model. Blowfish scored a rating of 7.89 at 100 MB and 16.45 at 500 MB, whereas DES achieved a value of 5.9 at 100 MB and 10.73 at 500 MB, respectively. The RC4 model scored 4.89 at 100 MB and 9.01 at 500 MB. The AES achieved the value of 2.48 at 100 MB and achieved the value of 8.84 at the data size 500 MB. When the data amount increased to 100 MB, the BC-XORECC model reached a value of 1.2 and it increased to 4.12 when the data size increased to 500 MB. When the data size is 100 MB, the proposed model achieves 0.67 and increases to 3.24 when the data size is 500 MB.

The throughput value of the proposed and existing model is shown in figure 8. The proposed model is compared

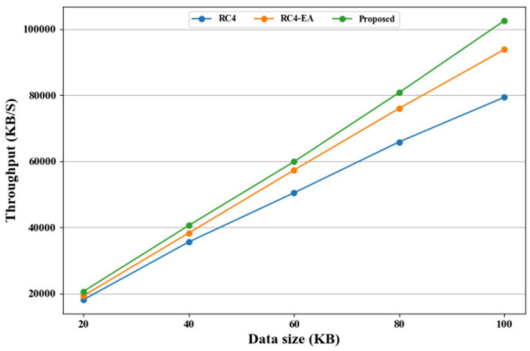

FIGURE 8. Throughput vs data size.

with existing models like RC4 and RC4-EA. The RC4 algorithm achieved the value of 18098.39 at 20 KB, 35552.48 at 40 KB, 50422.4 at 60 KB, 65844.64 for 80 KB and 79362.42 at 100 KB. The RC4-EA algorithm achieved the value of 19287.85 for 20 KB, 38277.92 for 40 KB, 57299.23 for 60 KB, 75983.77 at 80 KB and 93811.31 for 100 KB. The proposed model achieved the value of 21911.27 for 20 KB, 40301.93 for 40 KB, 58692.59 for 60 KB, 79021.71 for 80 KB and for 100 KB, the proposed model achieved a value of 95475.03 KB/s.

V. CONCLUSION

In this study, an elliptical crypt with secured blockchain-assisted Federated Q-Learning Framework is proposed. Data gathering, encryption, attack detection, safe storage and validation are all part of the proposed system. The input IoMT data are initially gathered from publically available datasets. Encryption is used to secure the provided inputs using the Extended Elliptic Curve Cryptography (E_ECurCypt) approach. This encrypted data is fed as an input to the proposed blockchain-powered collaborative learning model. The federated Q-Learning model processed the inputs and analyzed the attacks provided to ensure better privacy. Finally, the data is securely stored on decentralized blockchain technology. To validate the proposed architecture, the Delegated Proof of Stake (Del_PoS) consensus technique is used. The WUSTL-EHMS-2020 dataset is used to carry out the investigation. The performance of the proposed framework will be evaluated using multiple matrices and the results will be compared to other current approaches. The proposed model returned the following results: 99.23% accuracy, 98.42% precision, 98.12% recall, 98.27% F1 score, 59080.506 average throughput, 1.94 seconds average decryption time and 1.84 seconds average encryption time. Although there is potential to expand security and privacy in smart healthcare systems through the integration of elliptic cryptography with a secured blockchain assisted federated Q-learning framework, there are a few potential limitations to take into consideration. Initially, latency problems can be brought about by the processing expense of extended elliptic curve, which would affect the real-time responsiveness desirable in healthcare environments. Besides, the usage

of blockchain technology increases scalability problems as the transaction volume increases, and the size of blockchain also expands. This possibly demanding more processing and storage capacity. Additionally, maintaining data synchronization and consistency among dispersed nodes can provide problems for the federated learning technique, predominantly in heterogeneous healthcare environments with changing data formats and standards.

Subsequently, there are privacy concerns about storing sensitive medical records on a blockchain, since encrypted data might be vulnerable to attacks or other sophisticated data breaches that permit for unauthorized access or analysis. Thereby, even if the proposed framework improves security and collaborative learning, undertaking these concerns is indispensable to its successful application in intelligent healthcare systems. In the future, this research would want to add more complex assaults as well as more recent datasets to train the proposed algorithm. This research is interested in studying consensus mechanisms that can identify all assaults, including resend attacks and boost efficiency.

REFERENCES

[1] Y. Chang, C. Fang, and W. Sun, "A blockchain-based federated learning method for smart healthcare," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–12, Nov. 2021.

[2] A. Rahman, T. Debnath, D. Kundu, M. S. I. Khan, A. A. Aishi, S. Sazzad, M. Sayduzzaman, and S. S. Band, "Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities," *AIMS Public Health*, vol. 11, no. 1, pp. 58–109, 2024.

[3] C. U. O. Kumar, S. Gajendran, V. Balaji, A. Nhaveen, and S. S. Balakrishnan, "Securing health care data through blockchain enabled collaborative machine learning," *Soft Comput.*, vol. 27, no. 14, pp. 9941–9954, Jul. 2023.

[4] O. K. Cu, S. Gajendran, R. M. Bhavadharini, M. Suguna, and R. Krithiga, "EHR privacy preservation using federated learning with DQRE-Scnet for healthcare application domains," *Knowl.-Based Syst.*, vol. 275, Sep. 2023, Art. no. 110638.

[5] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS—A blockchain based approach for smart healthcare system," *Healthcare*, vol. 8, no. 1, Mar. 2020, Art. no. 100391.

[6] S. Otoum, I. Al Ridhawi, and H. T. Mouftah, "Preventing and controlling epidemics through blockchain-assisted AI-enabled networks," *IEEE Netw.*, vol. 35, no. 3, pp. 34–41, May 2021.

[7] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain and edge computing for decentralized EMRs sharing in federated healthcare," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[8] N. K. Al-Shammari, T. H. Syed, and M. B. Syed, "An edge—IoT framework and prototype based on blockchain for smart healthcare applications," *Eng., Technol. Appl. Sci. Res.*, vol. 11, no. 4, pp. 7326–7331, Aug. 2021.

[9] T. Veeramakali, R. Siva, B. Sivakumar, P. C. S. Mahesh, and N. Krishnaraj, "An intelligent Internet of Things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *J. Supercomput.*, vol. 77, no. 9, pp. 9576–9596, Sep. 2021.

[10] M. Khan and A. Malviya, "Big data approach for sentiment analysis of Twitter data using Hadoop framework and deep learning," in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng.*, Vellore, India, Feb. 2020, pp. 1–5, doi: 10.1109/ic-ETITE47903.2020.201.

[11] M. Khan, S. Hariharasitaraman, S. Joshi, V. Jain, M. Ramanan, A. SampathKumar, and A. A. Elngar, "A deep learning approach for facial emotions recognition using principal component analysis and neural network techniques," *Photogramm. Rec.*, vol. 37, no. 180, pp. 435–452, Dec. 2022, doi: 10.1111/phor.12426.

[12] R. Ch, G. Srivastava, Y. L. V. Nagasree, A. Ponugumati, and S. Ramachandran, "Robust cyber-physical system enabled smart healthcare unit using blockchain technology," *Electronics*, vol. 11, no. 19, p. 3070, Sep. 2022.

[13] C.-R. Shyu, K. T. Putra, H.-C. Chen, Y.-Y. Tsai, K. S. M. T. Hossain, W. Jiang, and Z.-Y. Shae, "A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications," *Appl. Sci.*, vol. 11, no. 23, p. 11191, Nov. 2021.

[14] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," *J. Healthcare Informat. Res.*, vol. 5, no. 1, pp. 1–19, Mar. 2021.

[15] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, and Y. Tang, "VFChain: Enabling verifiable and auditable federated learning via blockchain systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 173–186, Jan. 2022.

[16] W. Liu, Y. Zhang, G. Han, J. Cao, H. Cui, and D. Zheng, "Secure and efficient smart healthcare system based on federated learning," *Int. J. Intell. Syst.*, vol. 2023, pp. 1–12, Feb. 2023.

[17] M. Asad, M. Aslam, S. F. Jilani, S. Shaukat, and M. Tsukada, "SHFL: K-anonymity-based secure hierarchical federated learning framework for smart healthcare systems," *Future Internet*, vol. 14, no. 11, p. 338, Nov. 2022.

[18] C. Zhou, A. Fu, S. Yu, W. Yang, H. Wang, and Y. Zhang, "Privacy-preserving federated learning in fog computing," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10782–10793, Nov. 2020.

[19] S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. C. Arya, G. S. Wander, and R. Buyya, "HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments," *Future Gener. Comput. Syst.*, vol. 104, pp. 187–200, Mar. 2020.

[20] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of Health Things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020.

[21] S. Messaoud, A. Bradai, O. B. Ahmed, P. T. A. Quang, M. Atri, and M. S. Hossain, "Deep federated Q-learning-based network slicing for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5572–5582, Oct. 2020.

[22] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, "Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems," *Comput. Netw.*, vol. 197, Oct. 2021, Art. no. 108279.

[23] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102355.

[24] D. Połap, G. Srivastava, and K. Yu, "Agent architecture of an intelligent medical system based on federated learning and blockchain technology," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102748.

[25] P. Chinnasamy, A. Albakri, M. Khan, A. A. Raja, A. Kiran, and J. C. Babu, "Smart contract-enabled secure sharing of health data for a mobile cloud-based E-health system," *Appl. Sci.*, vol. 13, no. 6, p. 3970, Mar. 2023.

[26] S. Datta and S. Namasudra, "Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile edge computing," *IEEE Trans. Consum. Electron.*, early access, 2024.

[27] X. Zhang, K. Chen, J. Ding, Y. Yang, W. Zhang, and N. Yu, "Provably secure public-key steganography based on elliptic curve cryptography," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3148–3163, 2024.

[28] C. Liu, Y. Wang, C. Yang, and W. Gui, "Multimodal data-driven reinforcement learning for operational decision-making in industrial processes," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 1, pp. 252–254, Jan. 2024.

[29] D. O. Oyewola, S. A. Akinwunmi, and T. O. Omotehinwa, "Deep LSTM and LSTM-attention Q-learning based reinforcement learning in oil and gas sector prediction," *Knowl.-Based Syst.*, vol. 284, Jan. 2024, Art. no. 111290.

[30] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey," *Ad Hoc Netw.*, vol. 152, Jan. 2024, Art. no. 103320.

[31] H. M. Saleh, H. Marouane, and A. Fakhfakh, "Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning," *IEEE Access*, vol. 12, pp. 3825–3836, 2024.

[32] G. Verma, "Blockchain-based privacy preservation framework for healthcare data in cloud environment," *J. Experim. Theor. Artif. Intell.*, vol. 36, no. 1, pp. 147–160, Jan. 2024.
[33] K. Venkatesan and S. B. Rahayu, "Blockchain security enhancement: An approach towards hybrid consensus algorithms and machine learning techniques," *Sci. Rep.*, vol. 14, no. 1, p. 1149, Jan. 2024.

SUDHAKARAN GAJENDRAN received the B.Tech. degree in information technology from the Vel Tech Engineering College, Anna University, Chennai, in 2009, the M.E. degree in computer science and engineering from the Government College of Engineering, Tirunelveli, Anna University, in 2011, and the Ph.D. degree from the Department of Computer Science and Engineering, Anna University, in 2021. He is currently an Assistant Professor with the School of Electronics Engineering (SENSE), Vellore Institute of Technology, Chennai. He has been a Researcher in bioinformatics and artificial intelligence, since 2015. His current research is concerned with extracting and analyzing the association between different entities from the biomedical literature text and gene sequence analysis.

REVATHI MUTHUSAMY is currently working as an Assistant Professor (Sr. G) with the School of Computer Science Engineering, Vellore Institute of Technology Chennai Campus. She has been involved in research work in bio-informatics, path planning for autonomous underwater vehicles and generative AI. Her research interests include optimization systems for real world scenarios, computer vision and robotics.

KRITHIGA RAVI is currently an Assistant Professor (Sr. G) with the School of Computer Science Engineering, Vellore Institute of Technology, Chennai Campus. She is specialized in the domain of machine language, medical image processing, and natural language processing with the College of Engineering, Guindy, Anna University, Chennai, to obtain the Ph.D. degree. Her research achievements and activities include publishing articles in refereed journals with an H-index value of three. Her major research contributions have been published by SCI journals, such as *Journal Machine Vision and Application* (Springer), *Computer Communications* (Elsevier), *Computational Intelligence*, and *Concurrency and Computation* (Wiley). She has participated in and presented papers at international conferences.

OMKUMAR CHANDRAUMAKANTHAM received the B.Tech. and M.Tech. degrees (Hons.) in CSE from colleges affiliated to JNTU, Anantapur, in 2010 and 2013, respectively, and the Ph.D. degree from Anna University, Chennai, in 2020, with a specialized in the domain of cyber security. He is currently working as an Assistant Professor (Sr. G) with the School of Computer Science Engineering, Vellore Institute of Technology Chennai Campus.

SUGUNA MARAPPAN received the B.E. degree in CSE from the Kumaraguru College of Technology, Coimbatore, the M.E. degree in CSE from the Government College of Technology, Coimbatore, and the Ph.D. degree in information and communication engineering from Anna University, Chennai. She is an Assistant Professor Senior Grade-II at the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai. She has published more than 20 research articles in international journals and 15 international conferences. Her research interests include data analytics, health care analytics, cloud computing and agile project management. She is member of ISTE and IAENG.