IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 July 2024, accepted 19 August 2024, date of publication 22 August 2024, date of current version 2 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3447829

RESEARCH ARTICLE

Secure Federated Cloud Storage Protection Strategy Using Hybrid Heuristic Attribute-Based Encryption With Permissioned Blockchain

ATUL B. KATHOLE[1], KAPIL NETAJI VHATKAR[1], ANKUR GOYAL[2], SHIVKANT KAUSHIK[3], AMITA SANJIV MIRGE[4], PRINCE JAIN[5], MOHAMED S. SOLIMAN[6], (Senior Member, IEEE), AND MOHAMMAD TARIQUL ISLAM[7], (Senior Member, IEEE)

[1]Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri-Chinchwad, Pune 411018, India
[2]Department of Computer Science and Engineering, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, Maharashtra 412115, India
[3]Department of Computer Science and Engineering (AI & DS), Greater Noida Institute of Technology (GNIOT), Greater Noida, Uttar Pradesh 201310, India
[4]Department of IT, Pimpri Chinchwad College of Engineering, Pune 411044, India
[5]Department of Mechatronics Engineering, Parul Institute of Technology, Parul University, Vadodara, Gujarat 391760, India
[6]Department of Electrical Engineering, College of Engineering, Taif University, Taif 21944, Saudi Arabia
[7]Department of Electrical, Electronic and Systems Engineering, Faculty of Engineering and Built Environment, UKM, Bangi, Selangor 43600, Malaysia

Corresponding authors: Prince Jain (princeece48@gmail.com) and Mohammad Tariqul Islam (tariqul@ukm.edu.my)

This research was funded by the Universiti Kebangsaan Malaysia Research Grant through the Dana Padanan Kolaborasi (DPK) under the grant number DPK-2022-006. Also, the research was funded by Taif University, Saudi Arabia, Project No. (TU-DSPP-2024-11).

ABSTRACT The rapid growth of the Internet of Medical Things (IoMT) has introduced significant security and privacy challenges in managing and protecting medical data. This paper proposes a secure federated cloud storage system designed to address these challenges using a hybrid heuristic attribute-based encryption (ABE) scheme integrated with a permissioned Blockchain. The proposed system enhances data confidentiality and integrity by first collecting medical information and then encrypting it with ABE using an optimal key generated by the Hybrid Mexican Axolotl with Energy Valley Optimizer (HMO-EVO). The encrypted data is securely stored in a permissioned blockchain, ensuring robust access control and protection against data breaches. For effective healthcare monitoring, the system employs federated learning with a Multi-scale Bi-Long Short-Term Memory and Gated Recurrent Unit (MBiLSTM-GRU) to predict diseases accurately. This federated approach allows for decentralized training of deep learning models, preserving patient data privacy while leveraging collective learning. Experimental results show that the proposed system outperforms conventional methods in terms of security, efficiency, and predictive accuracy. This research offers a comprehensive framework for secure medical data management, combining the strengths of federated learning and blockchain technology to address the critical issues of data ownership, regulatory compliance, and privacy in IoMT networks.

INDEX TERMS Attribute-based encryption, blockchain technology, federated learning, health monitoring, IoMT security, optimal key generation.

I. INTRODUCTION

Cloud computing has become a popular framework for data storage due to its benefits, such as on-demand supply, reduced computational effort, low cost, and improved asset management, rapidly gaining popularity among users [1]. It offers service-oriented architectures like Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Infrastructure-as-a-Service (IaaS), where end-to-end reliability and quality are crucial due to fluctuating user dynamics [2]. The quality of

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

experience between cloud customers and service providers is evaluated based on the service level agreement [3], which measures factors such as repair time, uptime, mean time between failures, user responsibility, and response time [4]. Federated learning is employed to enhance security by enabling the training of a common global model on a centralized server while keeping data within the pertinent organizations, rather than aggregating data from multiple sources using conventional techniques. This method allows different regions to collaborate in training a global system without directly exchanging information, thereby enhancing individual privacy [5].

Privacy-related issues are exacerbated by attackers targeting gateway networks and servers, data forgery, record falsification, unauthorized device penetration, and device interference. Implementing a blockchain-based framework and unified cloud computing techniques can address these problems [6]. Blockchain technology, developed by Satoshi Nakamoto in 2008, includes a network of independent nodes that maintain a time-stamped collection of tamper-evident records [7]. It uses cryptography to secure data, ensuring decentralization, rigidity, and transparency [8]. Machine learning technology has found applications in various fields, including autonomous vehicles, smartphones, and embedded devices, offering a secure method for addressing privacy issues [9], [10].

Blockchain is also used for data protection in smart healthcare systems, regulating information dissemination, access to patient records, and other smart healthcare technologies [11]. It serves as the foundation for cybersecurity architecture in intelligent household networks within smart healthcare models [12]. Despite growing interest, research on smart healthcare technologies is spread across various disciplines [13]. This study aims to fill the knowledge gap and provide insights into blockchain technology and its applications in intelligent healthcare systems [14].

This paper introduces a trusted recommender system utilizing cloud techniques from multiple Fibre Channel Protocol (FCP) sites to the CU. At the middleware layer, the FCP-based protocol runs a ranking model to choose the best value for the CU [15]. The quality of experience and CU site manage payment services. The proposed outcomes showed high service quality. The file systems address the scalability limits of storing service offerings in the blockchain. The blockchain ledger is connected to the IPFS 32-bit hash, ensuring confidence, homogeneity, and data integrity. Hence, a secure federated cloud storage system with a disease detection component is developed to secure medical data in healthcare systems.

Most secure federated cloud storage systems are costly and suffer from misconfiguration, unauthorized access, lack of visibility, cyber-attacks, and insecure interfaces, leading to insufficient data governance and poor access control. Transactions are sometimes insecure. To resolve these challenges, various deep learning approaches have been designed for blockchain-based secure federated cloud storage systems. The features and challanges of these approaches are listed in Table 1.

Cloud Service Provisioning [16] improves bandwidth and decreases servicing latency, offering viable outcomes but suffering from trust issues and increased security vulnerabilities during data transactions. RTS-DELM [17] reduces computational burdens and implementation costs but maximizes latency and implementation time. Edge-cloud-AF [18] enhances data privacy and quality of service, increasing precision and F1-score, but suffers from malicious cyber attacks and security issues, lacking support for complex storage policies. Asynchronous aggregation [19] is less expensive and faster, reducing computational complexity but struggling with large data volumes and real-time applications. CNN [20] reduces security risks and provides better scalability, but is vulnerable to malicious gradient tampering and poisoning attacks, leading to unauthorized access. LSTM [21] offers flexible and manageable outcomes, improving early data breach detection but lacking early data security measures and reducing communication efficiency. Multi-tenant SaaS [22] protects data against internal and external threats, securing private data aggregation but failing to address severe privacy violations and data misuse, using low-quality models that decrease performance. SaaS [23] enhances transaction security and keeps records safe from malicious parties, improving immutability, transparency, and security, but not reducing business risk and incurring high monitoring and handling costs.

These disadvantages motivate the implementation of an effective blockchain-based secure federated cloud storage system with deep learning techniques [24]. The developed secure federated cloud storage system with health monitoring and disease detection aims to achieve several objectives. It is designed to effectively secure patient information and accurately predict diseases in hospitals through a secure federated cloud storage system with integrated health monitoring. The system utilizes ABE-based encryption with the HMO-EVO algorithm to optimally generate keys, thereby improving system efficiency by reducing memory size and computational time. Additionally, the HMO-EVO algorithm is employed for optimal key generation in ABE, ensuring high security and optimizing parameters such as activation function, number of epochs, and hidden neuron count in MBiLSTM-GRU to maximize accuracy, MCC, precision, and NPV in disease prediction. The performance of the proposed secure federated cloud storage system with health monitoring is examined against conventional models and algorithms using various performance metrics.

The developed secure federated cloud storage system with health monitoring is detailed in the following sections. Part II presents the proposed algorithm and dataset explanation. Part III describes the encryption process and optimal key generation. Part IV summarizes user authorization, federated learning, and the prediction approach. Part V provides a

summary of the experimental study of the developed secure federated cloud storage system. The concluding remarks of the proposed system are described in Part VI.

TABLE 1. Features and challenges of a secure federated cloud storage using cryptography.

Ref.	Methodology	Features	Challenges
Verma et al. [16]	Cloud Service Provisioning	Enhances bandwidth, decreases servicing latency, and provides viable outcomes.	Data is exchanged among heterogeneous stakeholders, leading to trust issues and increased security vulnerabilities.
Rehman et al. [17]	RTS-DELM	Decreases computational burdens of storage and reduces implementation cost.	Maximizes learning model latency and takes a lot of time for implementation.
Su et al. [18]	Edge-cloud-AF	Enhances data privacy, quality of service, and increases precision and F1-score measure.	Suffers from malicious cyber attacks, security-related issues, and lacks support for complex storage policies.
Jatain et al. [19]	Asynchronous aggregation	Less expensive, faster, and reduces computational complexity.	Hard to handle large amounts of data and struggles to predict for real-time applications.
Blanquer et al. [25]	CNN	Reduces security risks and provides better scalability.	Vulnerable to malicious gradient tampering, poisoning attacks, and unauthorized access.
Kumar et al. [21]	LSTM	Provides flexible, manageable outcomes and improves early detection of data breaches.	Lacks early data security measures and decreases communication efficiency.
Rafique et al. [22]	Multi-tenant SaaS	Protects data against internal and external threats and secures the aggregation of private data.	Does not address severe privacy violation, data misuse risks, and uses low-quality models, reducing performance.
Malomo et al. [23]	SaaS	Provides high security, ensuring data protection from hackers, and enhances immutability, transparency, and security.	Does not reduce business risk and incurs high costs for monitoring and handling the system.

II. BLOCKCHAIN-BASED CLOUD STORAGE PROTECTION FRAMEWORK USING FEDERATED LEARNING

A. SECURED HEALTHCARE DATA PROTECTION AND ANALYSIS SCHEME IN BLOCKCHAIN

Security and privacy are concerned with traditional cloud storage solutions, which is one of their biggest problems. They are giving a third-party supplier, who can have different rules and procedures, to access your data. The speed and latency of data operations provide another difficulty when employing cloud storage solutions. Although cloud storage may appear to be less expensive and simpler than local storage, there are additional expenses and considerations that are either hidden costs or variable costs. Since the price is exorbitant. Different cloud service providers could employ various standards and requirements for storing and accessing data, which might not be compatible with your current systems or applications. Advanced, reliable Cloud storage technologies and geographically dispersed data centers can make a provider into a failure and result in a disaster. Hence, the federated cloud storage system with disease detection is used to effectively secure the patient's information and accurately detect the disease. The blockchain based federated storage system still hard to handle the data security because of the data stolen by attackers. Some of the edge devices are lead to poison in the federated learning process. These medical data of edge devices are increasing the computing power of the federated learning storage system. It suffers from privacy protection key related issues during the data sharing process. The offered federated cloud storage system with health monitoring structural representation is depicted in Fig. 1.

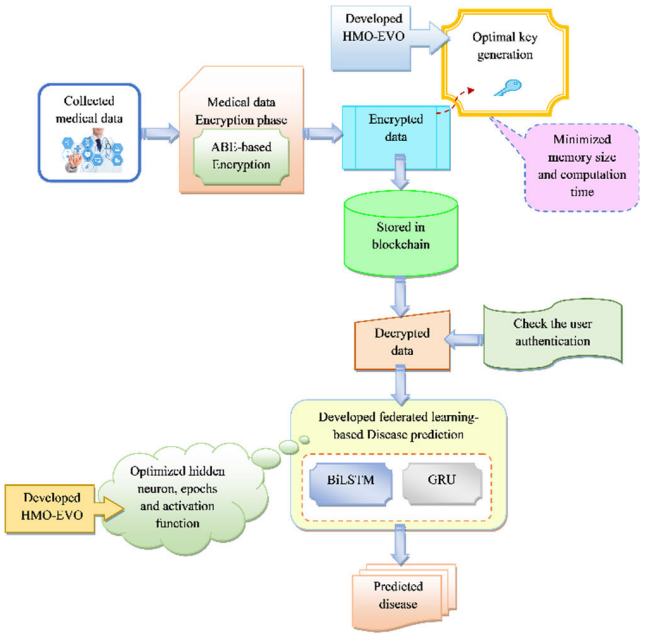

FIGURE 1. Structural representation of designed federated cloud storage system with health monitoring.

The newly implemented federated cloud storage system with health monitoring is used to effectively secure medical data from attackers and hackers and accurately predict disease. The medical information was gathered from online sources.Then, the medical data is fed into the encryption stage. The raw medical data is effectively encrypted and decrypted using ABE with optimal key and it is stored in the blockchain. Here, the investigated HMO-EVO strategy is employed to generate the optimal key for securing the data in terms of minimized memory size and computation time. It is effectively stored in the cloud because cloud storage

provides an additional layer of security against attackers and hackers. Then, the encrypted data is given to the prediction section. From the stored data, the health monitoring is effectively demonstrated to predict the disease using hybridized BiLSTM and GRU networks and it is named MBiLSTM-GRU. Here, the developed HMO-EVO strategy is utilized to optimized the values and the values are number of epochs, hidden neuron and activation function for maximizing the accuracy, precision, MCC and NPV. Finally, the implemented federated cloud storage system with health monitoring is contrasted to traditional approaches and strategies with respect to experimental analysis in terms of performance measures.

B. MEDICAL DATA COLLECTION

The input data for Dataset-1 (Diabetes) was gathered utilizing the dataset from [26]. This dataset contains patient details in 9 columns: glucose, outcome, blood pressure, diabetes pedigree function, insulin, skin thickness, age, BMI, and pregnancies. For Dataset-2 (Heart Disease), the information was collected by utilizing the dataset from [27]. This dataset contains 76 attributes and 14 columns. The numbers are set at 0 to 4 integer values, including patient details such as age, sex, and target. The collected health information inputs are indicated by F_d^{Hb} the total amount of data noted as D.

C. IMPLEMENTED HMO-EVO

The developed HMO-EVO algorithm is used to effectively generate the optimal key for minimizing memory size and computational time. It is utilized to enhance the data encryption process. The parameter optimization in MBiLSTM-GRU is performed using HMO-EVO to enhance the accuracy, precision, MCC and NPV. The MAO algorithm gives accurate results. It has a simple structure and a very fast implementation process. However, it suffers from a large amount of data implementation. The EVO algorithms advantages are it are straightforward structure, and effective implementation. Yet, it showed poor rates for the prediction, and time complexity during training. The designed HMO-EVO is investigated to beat the issues. The term PS is the updated position of the offered HMO-EVO. The term d_e is the candidate position obtained from MAO and it is noted by $P1$. The term y_j^k is the current position obtained from EVO and it is represented by $P2$. Updated location in the designed HMO-EVO is represented by PS based on the location of $P1$ and $P2$. The new position PS is estimated using an adaptive concept and it is measured using Eq. (1).

$$PS = 0.5 * P1 + 0.5 * P2 \tag{1}$$

Here, the MAO strategy location is indicated by d_e and the WWO strategy location is noted by y_j^k. The updated location is represented by PS.

MAO: This algorithm draws its inspiration from axolotl behaviour [28]. The axolotl's breeding, birth, aquatic habitat, and tissue repair are all elements that affect its inspiration process. The axolotl vectors are represented by J and the dimension is noted by D. The limit is set at $[no_e, ny_e]$. The term $Qo = \{W_1, \ldots, W_{ot}\}$ is the axolotl population size. Here, the size is represented by ot. These sizes are used to determine the best solution. The format of the vector is defined by $W_f \in Qo, \ 1 \leq f \leq ot$. The form of $W_f = [w_{f1}, \ldots, w_{fD}]$ is equal to $W_f \in Qo, \ 1 \leq f \leq ot$.

The four main phases are the passage from the larval state to adulthood, the damage stage and repair, the preproduction stage and assortment. Axolotl populations are started at random. The male and female populations are divided based on sex. The most effective person has superior camouflage, and the others will adjust their coloration in response. The colour changing behaviour is given in Eq. (2).

$$b_{fe} \leftarrow b_{fe} + \left(b_{ctu,e} - b_{fe}\right) * \vartheta \tag{2}$$

Here, the best male axolotl is noted by b_{ctu} and the present male axolotl is indicated by b_f. The female group of axolotl transforms from larvae into adults. That process is indicated in Eq. (3).

$$g_{fe} \leftarrow g_{fe} + \left(g_{ctu,e} - g_{fe}\right) * \vartheta \tag{3}$$

Here, the best female axolotl is noted by g_{ctu} and the current male axolotl is indicated by g_f. Some axolotl does not change their body and their colours. The random values are represented by $random \in [0, 1]$. The male group of axolotl optimization is measured using Eq. (4).

$$qo_f = \frac{jb_f}{\sum jb_f} \tag{4}$$

Here, the optimization value jb_f is used for male axolotl. The female group of axolotl optimization is calculated by Eq. (5).

$$qo_f = \frac{jg_f}{\sum jg_f} \tag{5}$$

Here, the term jg_f is the optimization value of female axolotl. The male axolotl behaviour is given in Eq. (6).

$$b_{fe} \leftarrow no_e + (ny_e - no_e) * se_e \tag{6}$$

The female axolotl behaviour is given in Eq. (7).

$$g_{fe} \leftarrow no_e + (ny_e - no_e) * se_e \tag{7}$$

The axolotl's damage region is denoted by Eqo. The axolotl is hurt by accident or moving across the water. This behaviour is called injury or restoration. The regeneration process of the axolotl is measured using Eq. (8).

$$qo'_{fe} \leftarrow no_e + (ny_e - no_e) * se_e \tag{8}$$

Here, the random value is noted by se_e. Hence, the best global solution is determined in the search phase.

EVO: The term "physical reaction" describes the creation of new particles by the collision of two particles or foreign subatomic particles [29]. Based on the particles, which are thought to increase forever, the vast majority of cosmos particles are considered unstable. This physics reaction behaviour is implemented using the EVO algorithm. The individual

candidate operation is indicated by y_j^k. The EVO initialization procedure is measured by Eq. (9).

$$y_j^k = y_{j,\min}^k + rnd.\left(y_{j,\max}^k - y_{j,\min}^k\right) \tag{9}$$

In the EVO, the dimension is represented by e. The total particles are noted by o. The initial location is denoted as y_j^k. The lower and upper level values are $y_{j,\min}^k$ and $y_{j,\max}^k$, respectively. The random value is noted by rnd. The term FC indicates the enrichment bound measured by Eq. (10).

$$FC = \frac{\sum_{j=1}^{o} OFM_j}{o} \tag{10}$$

Here, the enrichment bound is determined using the differences between neutron poor and neutron rich values. The particle's neutron enrichment stage is indicated by OFM. The objective function of the particle's stability stage is calculated by Eq. (11).

$$TM_j = \frac{OFM_j - CT}{XT - CT} \tag{11}$$

Here, the term TM is the particle's stability. The worst particles are denoted by XT and the best particles are noted by CT. If $OFM_j > FC$ then the particle is set to large value. The beta, gamma and alpha values are used in the decay process. The mathematical process of identifying new particles is given in Eq. (12).

$$y_j^{new-1} = y_j\left(Y_{CT}\left(y_j^k\right)\right) \tag{12}$$

Here, the stability best value is indicated by Y_{CT}. The present position is indicated by y_j^k. The nearest particles are noted by y_j. The term E_j^l is calculated using Eq. (13).

$$E_j^l = \sqrt{(y2 - y1)^2 + (z2 - z1)^2} \tag{13}$$

The j^{th} particle to l^{th} nearest particle distance is noted by E_j^l. Update the position using another candidate and this behaviour is calculated using Eq. (14).

$$y_j^{new-2} = y_j\left(Y_{OH}\left(y_j^k\right)\right) \tag{14}$$

Here, the new particle is indicated by y_j^{new-2} and the present location is denoted by y_j^k. This involves performing the highest level of center of the values as part of a procedure for updating the location of the particles. These algorithmic features imitate the values propensity to approach the stability band, where the majority of values are located and most of them have greater degrees of stability. The centre value of the particle is given in Eq. (15).

$$Y_{DQ} = \frac{\sum_{j=1}^{o} Y_j}{o} \tag{15}$$

Here, three position update processes are included in the algorithm's main loop. The updated new positions of the particle are indicated by Y_j^{new-1} and it is measured using Eq. (16).

$$Y_j^{new-1} = Y_j + \frac{\left(s_1 \times Y_{CT} - s_2 \times Y_{DQ}\right)}{TM_j} \tag{16}$$

The terms s_1 and s_2 are random variables. It is used to identify the movements of the particle. The mathematical process of updating another particle's location is given in Eq. (17).

$$Y_j^{new-2} = Y_j + \left(s_3 \times Y_{CT} - s_4 \times Y_{DQ}\right) \tag{17}$$

Here in the search space, the movement's values are set randomly. This mathematical process is given in Eq. (18).

$$Y_j^{new} = Y_j + s \tag{18}$$

Here, the terms Y_j^{new} and Y_j are updated location of the particles. The value is taken in the interval of [0, 1].

The tricky aspect of this approach in the exploration phase may direct the computer to regionally optimal solutions. The other phase seeks to fine-tune the regionally optimal candidates. The pseudo-code of implemented HMO-EVO is shown in Algorithm 1. Finally, the flowchart of implemented HMO-EVO is depicted in Fig. 2.

Algorithm 1 Investigated HMO-EVO

```
Load the particle's position and population
Calculate the fitness function values
Determine the particles 's enrichment bound
  While (iter < max _Iter)
  Determine the optimized male and female axolotl population
    For (K = 1 to MaxIter )
      For (M = 1 to Npop)
      Update the PS position employing the adaptive concept
                Update the position using MAO
                Evaluate the female axolotl position
                Determine the best position
                Generate the male axolotl position
      If (s ≤ eq )
                Update the position using EVO in Eq. (9)
                Finds the particle's stability stage
                Calculate the particle's position
                Generate the centre of the particle
      Else
                Calculate the particle's best stability
      End if
      End For
    End For
  Return stability solution
End
```

III. MEDICAL DATA DECRYPTION USING OPTIMAL GENERATED KEYS FOR SECURING CLOUD STORAGE RECORDS IN PERMISSIONED BLOCKS

A. ATTRIBUTE-BASED ENCRYPTION

The collected data is given to the ABE [30] encryption and it is noted by F_d^{Hb}. In Attribute-based Encryption (ABE), users may encrypt and decode data depending on client attributes. ABE is a vision of encryption with public key. One pairing procedure is needed for each decryption in many real-world ABE systems. The attribute-based encryption achieved high fine-grained access and flexible over the traditional models.

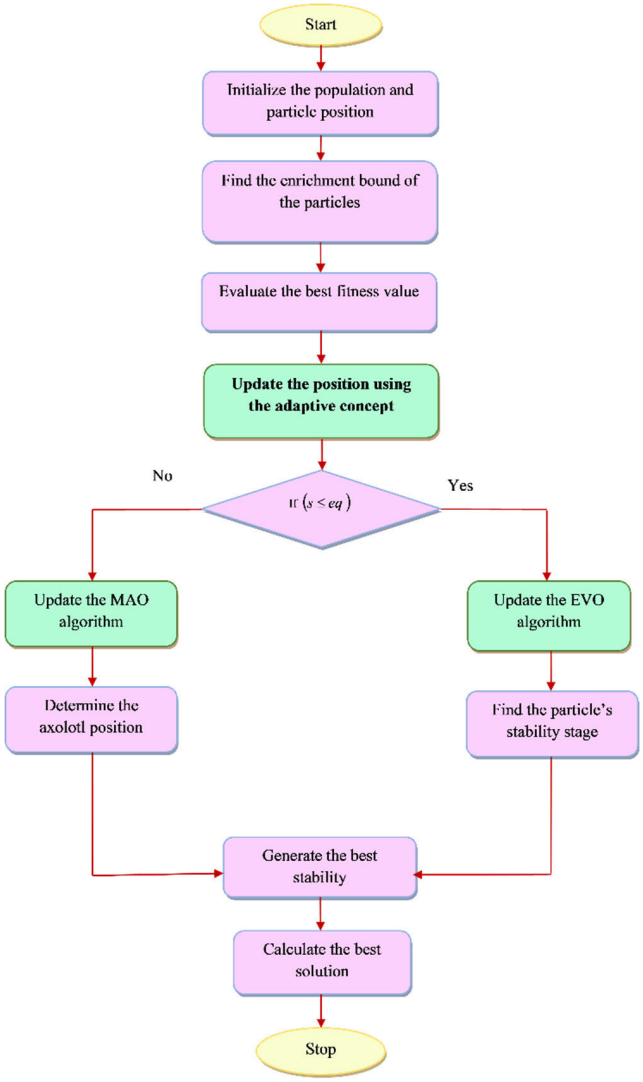

FIGURE 2. A flowchart of implemented HMO-EVO.

Algorithm

Setup (L): The procedure used by the attribute authority to set up the system chosen the L security value. Primary secret key is NL and the public key is QL that are the outputs.

Key-Gen (NL, T): The attribute authority's key generation method generates the secret attribute keys TL for the signer using the primary secret key NL and a set of attributes T as inputs.

Sign (QL, N, Q, and TL): The signing is the process used by a signer to produce a message's signature TU using inputs QL, a message N, an access policy Q, and attribute secret keys TL.

Verify (QL, N, Q, and TU): The algorithm used for validating is one that a verifier runs on the inputs QL, N, Q, and TU for a signature, an access policy, and a message. The result is true if TU is a legitimate signature from a vocalist whose qualities fulfil Q. The encrypted data is represented by BC_m^{En}. The diagrammatic representation of ABE-based encryption is depicted in Fig. 3.

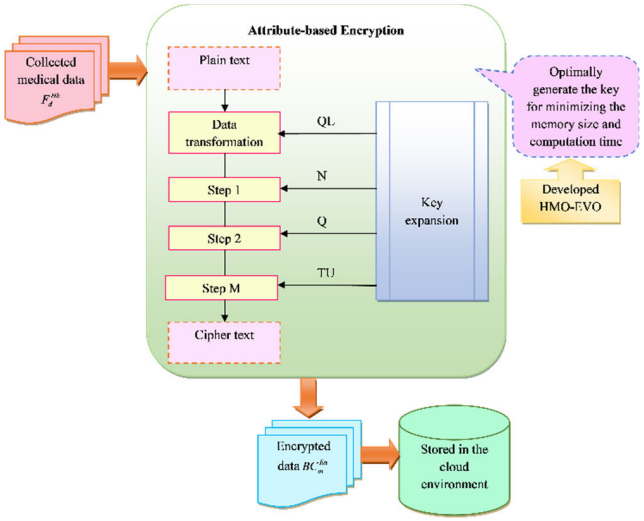

FIGURE 3. A basic diagram of ABE-based encryption.

B. OPTIMAL KEY GENERATION FOR DATA ENCRYPTION

The optimal key is used to secure the data very effectively. The developed HMO-EVO algorithm is used to effectively generate the optimal key for minimizing the computational time and memory size to enhance the system's effectiveness. The objective function formula is given in Eq. (19).

$$OJ_1 = \arg\min_{\left\{YE_{ABE}^{Key}\right\}} (Time + M\_size) \tag{19}$$

Here, the term YE_{ABE}^{Key} is the optimal key and it is generated in binary format and it is chosen in the interval of [0, 1]. The computational time is given in Eq. (20).

$$Time = EX * \frac{TM}{clock\_rate} \tag{20}$$

Here, the unit per execution rate is denoted by EX. The term $clock\_rate$ is the total execution rate. The term TM is the total execution time. The formula memory size calculation is measured by Eq. (21).

$$M\_size = 2^n * \frac{block\_size}{t\arg et\_size} + 1 \tag{21}$$

Here, the term $block\_size$ is the total value of blocks. The target size is noted by $t\arg et\_size$.

C. ENCRYPTED DATA STORAGE IN BLOCKCHAIN

In the blockchain, a procedure is used to split up the files. To avoid data loss during the data transmission, each data is assumed to be same value and it takes a copy for all files. Then, a key encrypts the folders, making nodes to others. Although blockchain technology was first used to store public data, developments have allowed for storing encrypted private data on the blockchain. Encrypting the files and distributing them over the decentralized network makes it more difficult for hackers to access the data, which is a benefit of using blockchain storage for encrypted data. No central

authority overseeing file access or holding the keys required to unlock the data exists. A hash task converts the letters to numbers that is an encrypted output. It is used to ensure data contained in the blocks on a blockchain are not altered. It provides high security to the data.

IV. USER AUTHORIZATION WITH FEDERATED LEARNING-BASED HEALTHCARE MONITORING SYSTEM

A. USER AUTHORIZATION

The user authentication is one of the networks that effectively verifies the client's verification. It is used to check the personal identification and verify the access of the individual person. By preventing unauthorized users from obtaining access and perhaps causing system damage, information theft, or other issues, it helps to guarantee that only authorized users may access a system. The quantity of private authorities on the system is decreased by authorization lists. It aids in boosting the system's security.

B. FEDERATED LEARNING FOR SECURED HEALTHCARE SYSTEM

Federated learning enables different locations to participate in the global model's training. Without explicitly exchanging datasets, federated learning incorporates implementing the blockchain network model. As a consequence, a central server host enhances the performance using a deep learning model. In order to preserve data localization at various places, the system is implemented by distributing itself over data centers, which include medical institutions or hospitals. No participant's data is shared or exchanged throughout the training process. As opposed to deep classical learning, which sends data to a single server, globally shared architecture is maintained by the server and is available to all universities. After that, each institute uses the model's error gradient to communicate with the server. All participant feedback is gathered by the central server, which then adjusts the global model in accordance with predetermined standards. By using the pre-established criteria, the model can assess the quality of the answer and only incorporate useful data. The organizations feedback given subpar or atypical outcomes may therefore go unnoticed. This technique produces a single cycle, which is then repeated until the blockchain network system is learned. The federated learning for the secured healthcare system diagram is depicted in Fig. 4.

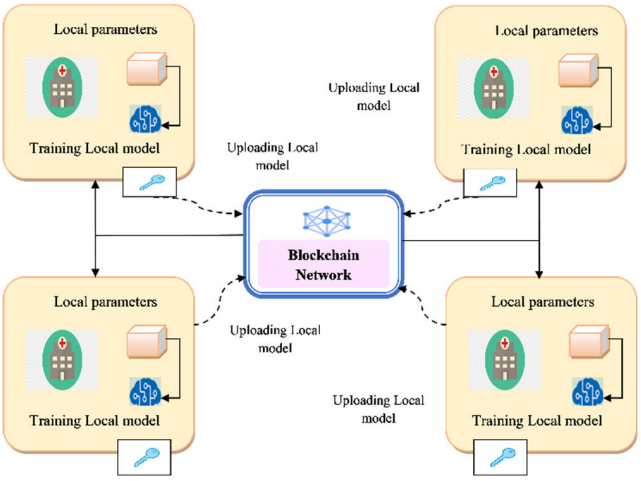

FIGURE 4. A diagrammatic representation of the federated learning model for the secured healthcare system.

C. MBiLSTM-GRU-BASED HEALTHCARE MONITORING

The developed MBiLSTM-GRU-based network is used to accurately predict the disease. It is used to reduce the death rates. The parameters such as activation function, number of epochs and hidden neuron count are optimized from LSTM and GRU using developed HMO-EVO algorithm for enhancing the prediction performance. Parameter optimization is used to increase the precision, accuracy, MCC and NPV value in the prediction section. The BiLSTM model effectively predicts the data with time series. It increases loyalty rates and customer satisfaction rates. But, it suffers from storage related problems. The GRU model provided fast performance and less memory during the training and also it easily handled the large amount of data. But, it gives low prediction rates and slow convergence rates. The objective function is calculated using Eq. (22).

$$OJ_2 = \underset{\left\{\begin{matrix} PT_{LSTM}^{hidden}, JU_{LSTM}^{epoch}, LM_{LSTM}^{Act} \\ GD_{GRU}^{hidden}, RV_{GRU}^{epoch}, CH_{GRU}^{Act} \end{matrix}\right\}}{\arg\min} \left(\frac{1}{A} + \frac{1}{pr} + \frac{1}{M} + \frac{1}{npv}\right) \tag{22}$$

In LSTM, the optimized hidden neuron count is indicated by PT_{LSTM}^{hidden} and it is chosen in the interval of [5, 255]. The number of epoch is optimized and it is represented by JU_{LSTM}^{epoch} in the interval of [5, 50]. The optimized activation function is denoted by LM_{LSTM}^{Act} and it is chosen in the interval of [1, 5]. In GRU, the optimized hidden neuron count is indicated by GD_{GRU}^{hidden} and it is chosen in the interval of [5, 255]. The number of epoch is optimized and it is represented by RV_{GRU}^{epoch} in the interval of [5, 50]. The optimized activation function is denoted by CH_{GRU}^{Act} and it is taken in the interval of [1, 5]. The formula of MCC is calculated using Eq. (23).

$$M = \frac{MI_o \times MI_k - MI_o \times TC_v}{\sqrt{\left(MI_o + TC_j\right)\left(MI_o + TC_v\right)\left(MI_k + MI_o\right)\left(MI_k + TC_v\right)}} \tag{23}$$

The precision formula is calculated using Eq. (24)

$$pr = \frac{MI_k}{MI_o + TC_v} \tag{24}$$

The NPV value is measured using Eq. (25)

$$npv = \frac{TC_v}{TC_v + MI_o} \tag{25}$$

The formula of accuracy is calculated using Eq. (26).

$$A = \frac{(TC_v + MI_o)}{(TC_v + MI_o + TC_j + MI_k)} \tag{26}$$

Here, the true positive and negative values are represented by the terms TC_v and TC_j, respectively. The false negative and positive values are noted by the terms MI_o and MI_k, respectively. The diagrammatic representation of the MBiLSTM-GRU-based healthcare monitoring system is depicted in Fig. 5.

D. BiLSTM

The encrypted data is given to the BiLSTM [31] network and it is denoted by BC_m^{En}. An important application for the BiLSTM is natural language processing. By linking the two hidden layers to the same output layer and processing time series information in both reverse directions and forward using two distinct hidden layers on the basis of LSTM, BiLSTM may store both earlier and later information. So, compared to uni-direction LSTM, theoretical prediction performance is superior. The forward and backward hidden layer activation outputs are included in BiLSTM's hidden layer output. The BiLSTM process is calculated using Eq. (27), Eq. (28) and Eq. (29), respectively.

$$\overrightarrow{i}_{u=} = \beta\left(X_{y\overrightarrow{i}} y_u + X_{y\overrightarrow{i}} \overrightarrow{i_{u-1}} + c_{\overrightarrow{i}}\right) \tag{27}$$

$$\overleftarrow{i}_{u=} = \beta\left(X_{y\overleftarrow{i}} y_u + X_{y\overleftarrow{i}} \overleftarrow{i_{u-1}} + c_{\overleftarrow{i}}\right) \tag{28}$$

$$I_{u=} = X_{y\overrightarrow{i}} \overrightarrow{i} + X_{y\overleftarrow{i}} \overrightarrow{i} + c_z \tag{29}$$

Here, the output is determined by upgrading forward and backward structures. The diagrammatic representation of LSTM system is depicted in Fig. 6.

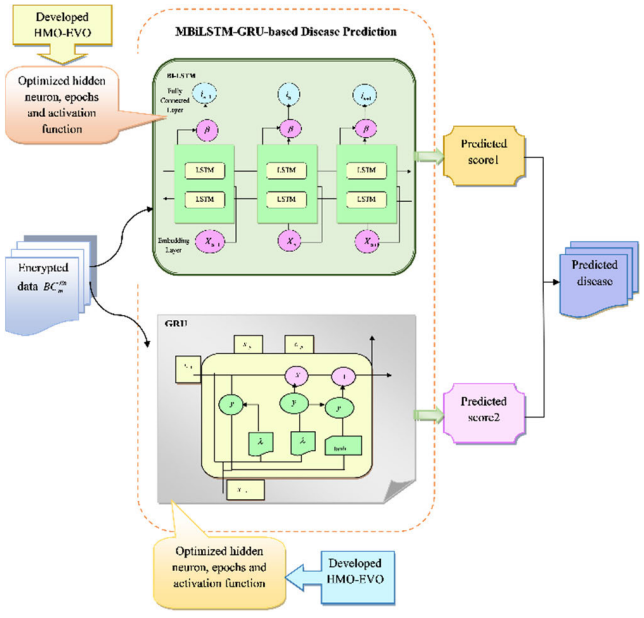

FIGURE 5. The diagrammatic representation of the MBiLSTM-GRU-based healthcare monitoring system.

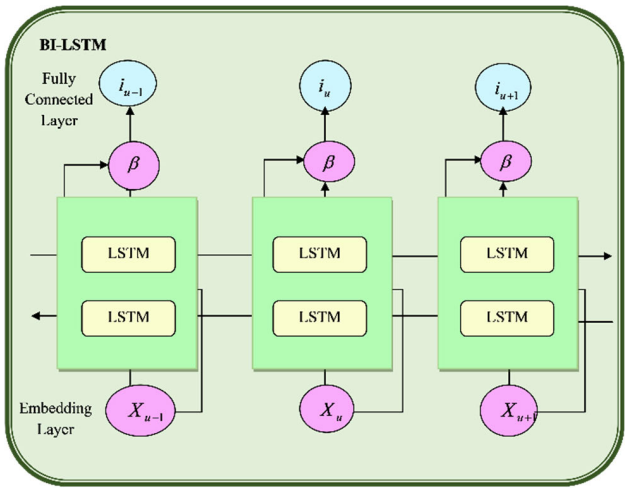

FIGURE 6. A basic diagram of the BiLSTM model.

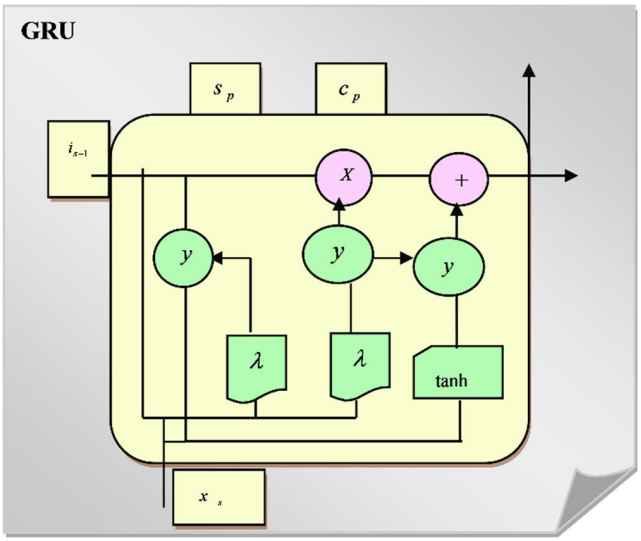

FIGURE 7. A basic diagram of the GRU system.

E. GRU

The encrypted data is given to the GRU [32] network and it is denoted by BC_m^{En}. Most of the models are used to predict the associated Sudden Death Syndrome (SDS) from a single spectral measurement. Multiple images of the same quadrate taken at various periods may improve the model's prediction accuracy. Consequently, a technique is used with time-series imaging is requirement. The processing of nonlinear time-series data is ideal for RNNs. When working with time-series information, the RNN might be revealed as the optimal component. The hidden layers of GRU are measured by Eq. (30).

$$y_{p=} = h\left(s_p * W_{iy}\right) \tag{30}$$

The GRU output layers are measured using Eq. (31).

$$s_p = g\left(x_p * W_{sx} + s_{p-1} * w_{ss}\right) \tag{31}$$

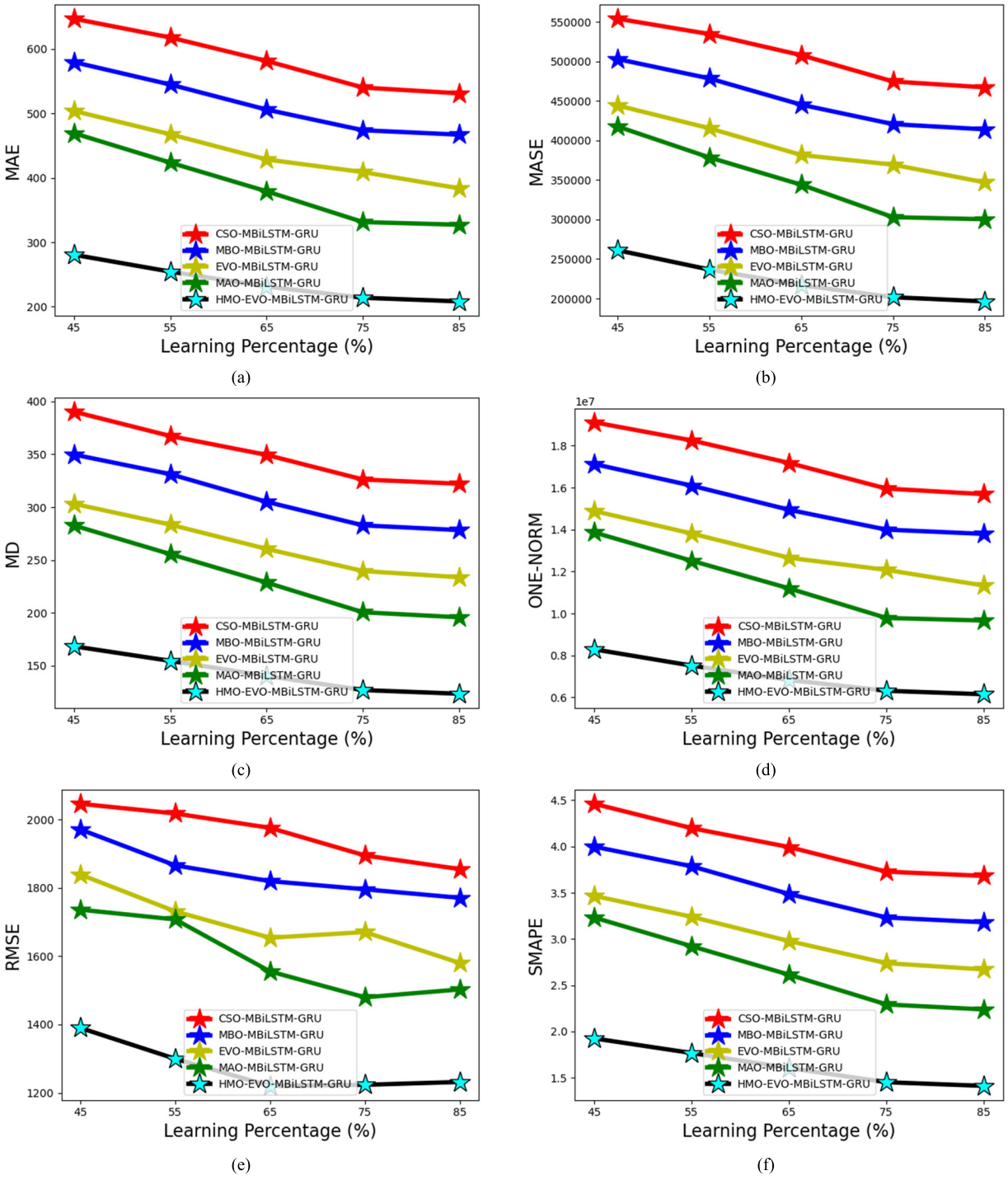

FIGURE 8. Effectiveness validation on developed federated cloud storage with health monitoring system among various algorithms with respect to (a) MAE (b) MASE (c) MD (d) ONE-NORM (e) RMSE and (f) SMAPE.

The gradient vanishing problem is resolved by the RNN approach, which is simple to implement. The term c_p is measured using Eq. (32).

$$c_p = \lambda \left(W_c \bullet \left[i_{p-1}, y_p \right] \right) \tag{32}$$

The term rp is calculated using Eq. (33).

$$rp = \lambda \left(W_r \bullet \left[i_{p-1}, y_p \right] \right) \tag{33}$$

Here, the term present input is noted by y_p. The output parameter is indicated by i_p. The individual hidden layer is noted by h'_p and it is given in Eq. (34).

$$h'_p = \tanh \left(W \bullet \left[r_p * i_{p-1}, y_p \right] \right) \tag{34}$$

Here, the GRU's random numbers are represented by c_p and i'_p, respectively.

$$i_p = \left(1 - c_p \right) * i_{p-1} + c_p * i'_p \tag{35}$$

The basic of diagram GRU system is depicted in Fig. 7.

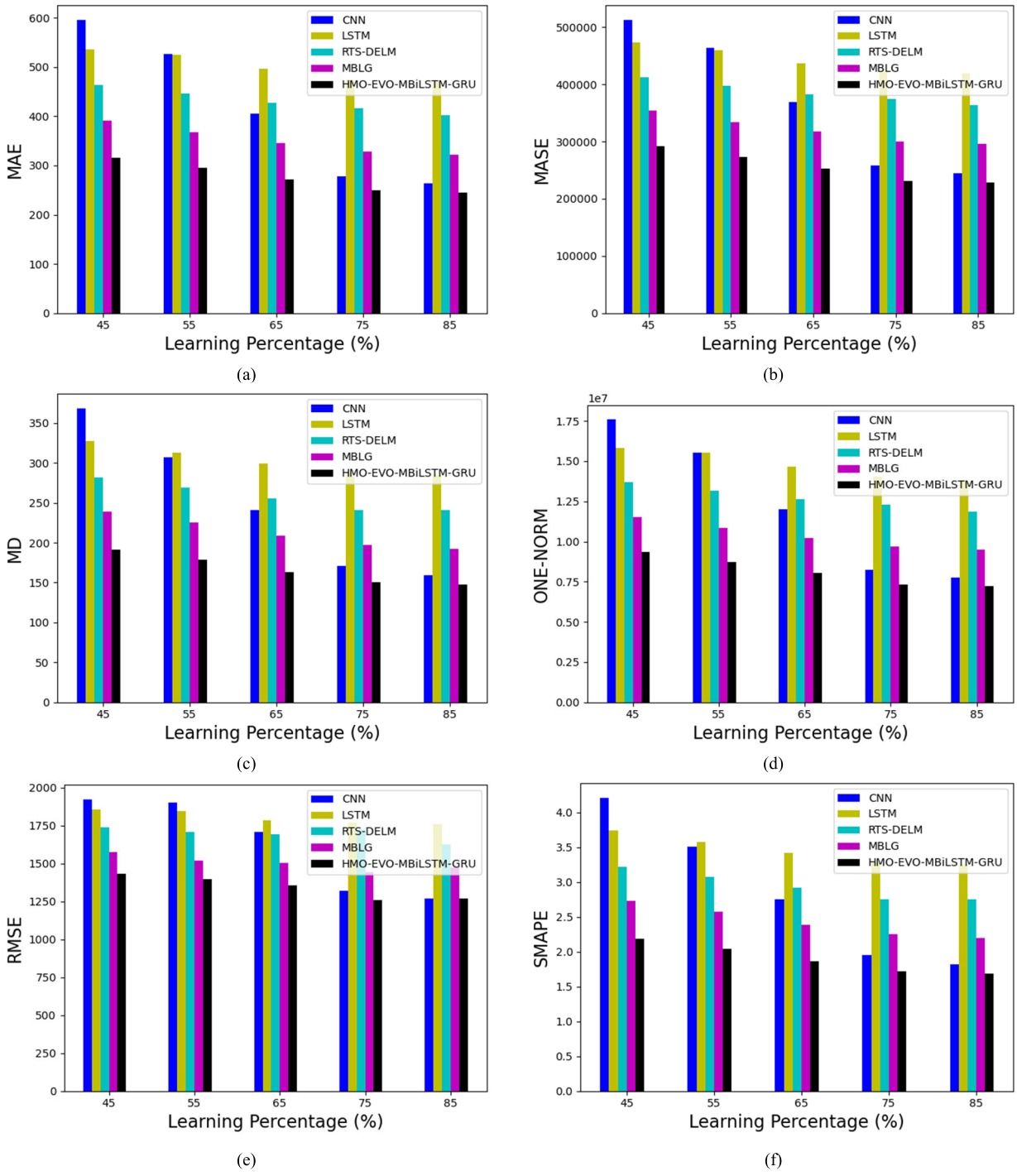

FIGURE 9. Performance evaluation on investigated federated cloud storage with health monitoring system among several approaches with respect to (a) MAE (b) MASE (c) MD (d) ONE-NORM (e) RMSE and (f) SMAPE.

V. RESULTS AND DISCUSSIONS

A. EXPERIMENTAL SETUP

The investigated federated cloud storage model with health monitoring was employed for securing the health data and it was executed by Python. The performance of the suggested federated cloud storage system with health monitoring was compared with various existing techniques and heuristic algorithms in terms of performance measures. A population size of 10, a maximum iteration of 50 and chromosomal length of 16 were used for the estimation study. The existing approaches such as Data Encryption Standard (DES) [33], Advanced Encryption Standard (AES) [34], Elliptic Curve Cryptography (ECC) [35] and ABS [30] were used. The algorithms such as Cat Swarm Optimization (CSO) [36],

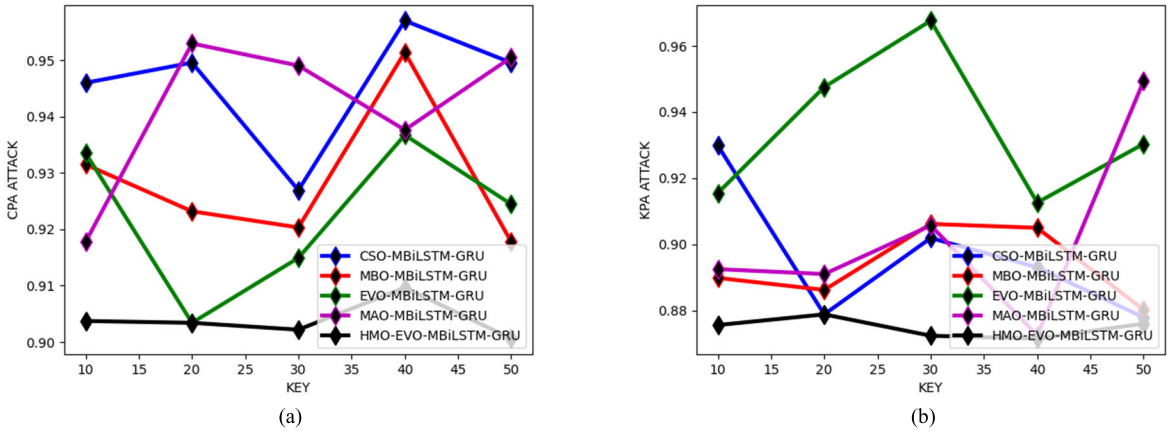

FIGURE 10. Performance analysis on offered federated cloud storage with health monitoring system among different algorithms with respect to (a) CPA attack and (b) KPA attack.

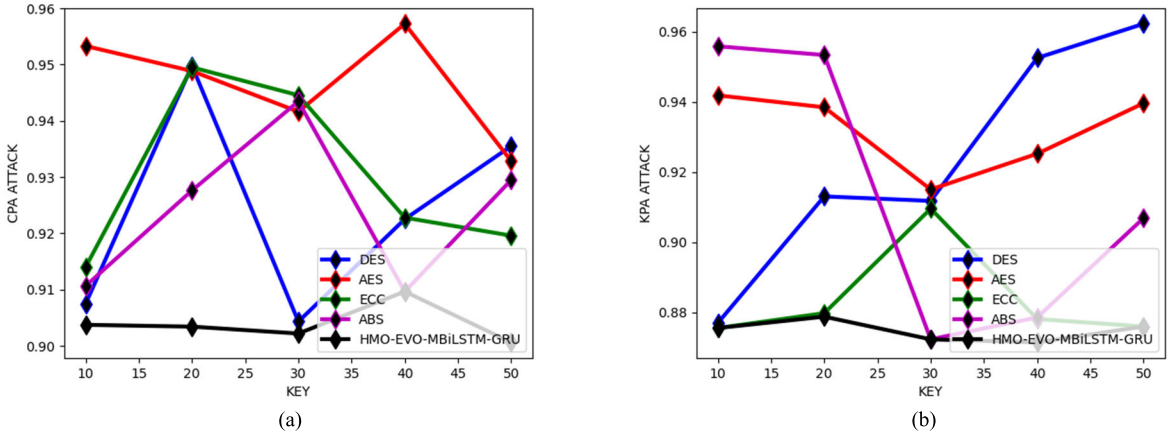

FIGURE 11. Performance validation on designed federated cloud storage with health monitoring model over various approaches with respect (a) CPA attack and (b) KPA attack.

Monarch butterfly optimization (MBO) [37], EVO [28] and MAO [29] were used for the experimental analysis.

B. EVALUATION MEASURES

The performance measures utilized for the federated cloud storage system are given below.

(a) ONE-NORM: It is calculated using Eq. (36).

$$Norm = \sum_{k} |N_k| \tag{36}$$

(b) RMSE: The RMSE value is calculated by Eq. (37).

$$M = \sqrt{\frac{\sum_{k=1}^{k} (cx_{k2} - hx_{k1})^2}{k}} \tag{37}$$

(c) TWO-NORM: It is measured using Eq. (38).

$$Norm2 = \left(\sum_{k=1}^{k} N_k^2 \right) \tag{38}$$

(d) MEP: The MEP value is given in Eq. (39).

$$P = \frac{100\%}{l} \sum_{k=1}^{k} \frac{cx - hx}{cx} \tag{39}$$

(e) MASE: The MASE parameter is measured by Eq. (40).

$$S = Mean \left(\frac{|hx|}{\frac{1}{l=1} \sum_{k=1}^{l} |cx_k - hx_{l-1}|} \right) \tag{40}$$

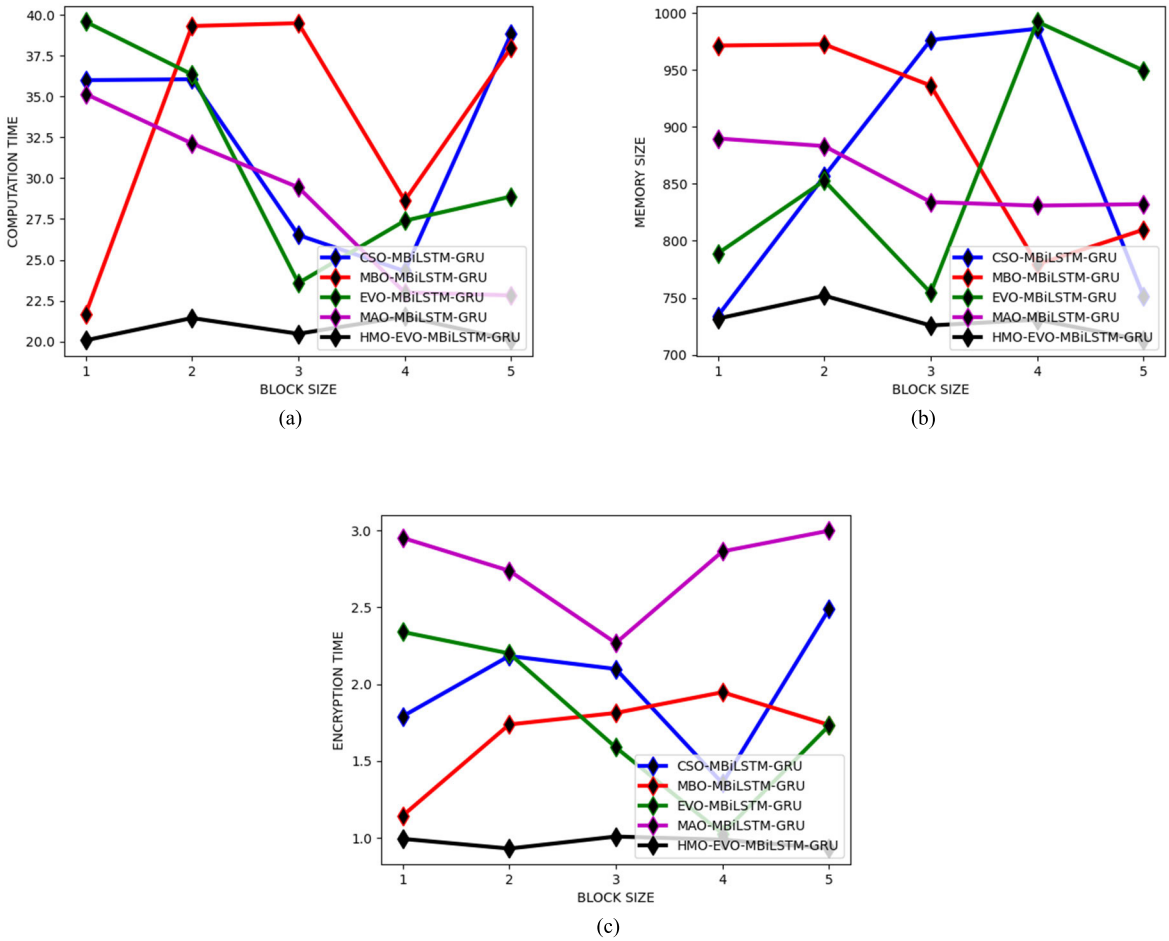

FIGURE 12. Performance analysis on implemented federated cloud storage with health monitoring model over different algorithms with respect to (a) Computational time (b) Memory size and (c) Encryption time.

(f) MAE: It is calculated using Eq. (41).

$$E = \frac{\sum_{k=1}^{l} |hx_k - cx_k|}{l} \tag{41}$$

(g) Infinity-Norm: It is measured by Eq. (42).

$$FI = \underset{1 \le k \le l}{Max} |N_k| \tag{42}$$

C. PERFORMANCE ANALYSIS OVER FEDERATED CLOUD STORAGE SYSTEM

The developed federated cloud storage with health monitoring model performance was compared to several heuristic strategy is depicted in Fig. 8. Also, the performance is compared to various techniques and it is shown in Fig. 9. The HMO-EVO-MBiLSTM-GRU-based federated cloud storage system with health monitoring given less MASE value of 41% than CSO, 47% than MBO, 54% than EVO, and 58% than MAO at the learning percentage of 65 from algorithm comparison. The implemented HMO-EVO-MBiLSTM-GRU-based federated cloud storage system with health monitoring to previous models and it is achieved better outcomes with less MASE.

D. CPA AND KPA EVALUATION OVER FEDERATED CLOUD STORAGE SYSTEM

The developed HMO-EVO-MBiLSTM-GRU-based federated cloud storage system with health monitoring performance in terms of CPA and KPA analysis over various heuristic strategies is shown in Fig. 10 and the comparison among existing methods is shown in Fig. 11. The HMO-EVO-MBiLSTM-GRU-based federated cloud storage with health monitoring model given less CPA attack value of 1.3% than CSO, 13.22% than MBO, 5.26% than EVO, and 6.25% than MAO at a key value of 30. Hence, the developed federated cloud storage system with a health monitoring system over the existing models showed greater performance in terms of CPA attack.

E. TIME ANALYSIS OVER FEDERATED CLOUD STORAGE SYSTEM

The developed federated cloud storage with health monitoring model performance was compared to several heuristic

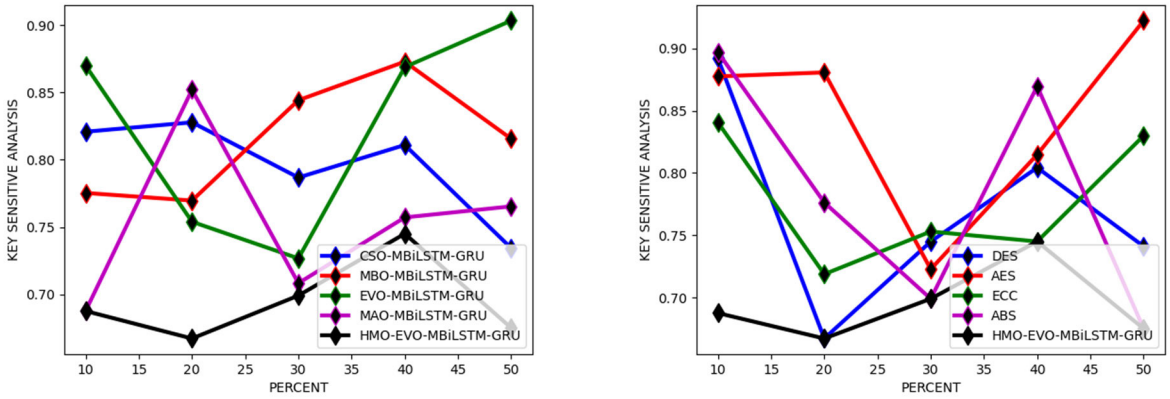

FIGURE 13. Performance analysis on designed federated cloud storage with health monitoring system over various algorithms and methods.

algorithms and it is depicted in Fig. 12 using computational time, memory size and encryption time analysis. The HMO-EVO-MBiLSTM-GRU-based federated cloud storage with a health monitoring system given less memory size of 2.6% than CSO, 12.9% than MBO, 21.2% than EVO, and 22.9% than MAO at the block size of 3 from algorithm comparison. The developed HMO-EVO-MBiLSTM-GRU-based federated cloud storage with a health monitoring system compared to traditional systems and it showed better results in terms of minimized computation time.

F. KEY SENSITIVITY AND KPA ANALYSIS OVER FEDERATED CLOUD STORAGE SYSTEM

The developed HMO-EVO-MBiLSTM-GR-based federated cloud storage with health monitoring system key sensitivity analysis is compared to various heuristic algorithms and conventional methods and it is shown in Fig. 13. The HMO-EVO-MBiLSTM-GRU-based federated cloud storage with health monitoring system given less key sensitivity value of 15% than CSO, 22% than MBO, 27% than EVO, and 33% than MAO over the percent value of 30 from the algorithm comparison. Hence, the developed HMO-EVO-MBiLSTM-GRU-based federated cloud storage with a health monitoring system over the existing models showed greater performance in terms of key sensitivity analysis.

G. OVERALL ANALYSIS ON THE DEVELOPED FEDERATED CLOUD STORAGE WITH THE DISEASE DETECTION SYSTEM

The performance comparison among investigated HMO-EVO-MBiLSTM-GRU-based federated cloud storage with health monitoring system with heuristic algorithms is given in Table 2 and also comparison among conventional approaches is given in Table 3. The HMO-EVO-MBiLSTM-GRU-based federated cloud storage with health monitoring system provided high MASE of 33% than CSO, 45% than MBO, 52% than EVO, and 57% than MAO. The implemented HMO-EVO-MBiLSTM-GRU-based federated cloud storage with health monitoring system achieved better efficacy than traditional approaches.

TABLE 2. Performance analysis of the developed Federated Cloud Storage with health monitoring system over algorithms.

Terms	CSO [36]	MBO [37]	EVO [28]	MAO [29]	HMO-EVO-MBiLSTM-GRU
MD	3.26	2.82	2.39	2.00	1.27
SMAPE	0.03	0.03	0.02	0.02	0.01
MASE	4745.10	4205.83	3693.37	3028.92	2016.84
MAE	5.40	4.74	4.08	3.31	2.13
RMSE	18.95	17.96	16.70	14.79	12.23
ONE-NORM	159548.9	139977.1	120777.3	97854.32	63129.66
TWO-NORM	3256.96	3086.58	2871.26	2542.82	2102.39
INFINITY-NORM	429.75	436.75	411.5	398.75	394.25

TABLE 3. Performance analysis of the developed Federated Cloud Storage with health monitoring system over techniques.

Terms	DES [33]	AES [34]	ECC [35]	ABS [30]	HMO-EVO-MBiLSTM-GRU
MD	1.71	2.87	2.41	1.97	1.27
SMAPE	0.01	0.03	0.02	0.02	0.014
MASE	2577.77	4216.07	3740.12	2997.92	2016.84
MAE	2.78	4.74	4.15	3.27	2.13
RMSE	13.19	17.67	17.24	14.41	12.23
ONE-NORM	82195.53	140198.5	122759.4	96675.94	63129.66
TWO-NORM	2267.36	3036.68	2963.26	2476.99	2102.39
INFINITY-NORM	369.25	407.5	479.25	368.5	394.25

VI. CONCLUSION

The newly implemented deep learning-based federated cloud storage with a health monitoring system was used to effectively secure the data and accurately predict the disease

from attackers. The medical data were collected from online databases. Next, the gathered data was collected from the internet. The medical data was fed into the ABE-based with optimal key encryption section. The data was effectively encrypted and decrypted, and stored in the blockchain. Here, the designed HMO-EVO strategy was employed to generate the optimal key for minimizing the memory size and computation time. Then, the encrypted data was given to the prediction section. Here, the disease was effectively predicted using BiLSTM and GRU networks, named MBiLSTM-GRU. Here, the developed HMO-EVO algorithm was utilized to optimize the parameters like hidden neuron, activation function, and the number of epochs for maximizing the accuracy, precision, MCC, and NPV. The HMO-EVO-MBiLSTM-GRU-based federated cloud storage with health monitoring system provided less MASE of 32% than DES, 46% than AES, 52% than ECC, and 21% than ABS. Finally, the implemented federated cloud storage with health monitoring system was compared to conventional approaches and algorithms with some effectiveness measures analysis, and it was given better efficacy with less MASE value. However, the system's reliance on specific datasets and the potential computational overhead in real-time applications may limit its scalability and applicability in diverse healthcare settings. Future research could explore integrating more varied datasets and optimizing the system's computational efficiency to enhance its adaptability and performance in broader contexts.

ACKNOWLEDGMENT

The authors would like to acknowledge to the Universiti Kebangsaan Malaysia Research Grant through the Dana Padanan Kolaborasi (DPK) under the grant number DPK-2022-006. Also, extend their appreciation to Taif University, Saudi Arabia, for supporting this work through project number (TU-DSPP-2024-11).

REFERENCES

[1] B. Sengupta, A. Dixit, and S. Ruj, "Secure cloud storage with data dynamics using secure network coding techniques," *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 2090–2101, Jul. 2022, doi: 10.1109/TCC.2020.3000342.

[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with secure network coding," *IEEE Trans. Comput.*, vol. 65, no. 6, pp. 1936–1948, Jun. 2016, doi: 10.1109/TC.2015.2456027.

[3] D. Seo, S. Kim, and G. Song, "Mutual exclusion method in client-side aggregation of cloud storage," *IEEE Trans. Consum. Electron.*, vol. 63, no. 2, pp. 185–190, May 2017, doi: 10.1109/TCE.2017.014838.

[4] B. Hong and W. Choi, "Optimal storage allocation for wireless cloud caching systems with a limited sum storage capacity," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6010–6021, Sep. 2016, doi: 10.1109/TWC.2016.2577025.

[5] P. Jain, M. T. Islam, and A. S. Alshammari, "Comparative analysis of machine learning techniques for metamaterial absorber performance in terahertz applications," *Alexandria Eng. J.*, vol. 103, pp. 51–59, Sep. 2024, doi: 10.1016/j.aej.2024.05.111.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011, doi: 10.1109/TPDS.2010.183.

[7] Y.-L. Lai and J. Cheng, "A cloud-storage RFID location tracking system," *IEEE Trans. Magn.*, vol. 50, no. 7, pp. 1–4, Jul. 2014, doi: 10.1109/TMAG.2014.2303810.

[8] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *IEEE Trans. Cloud Comput.*, vol. 6, no. 4, pp. 1136–1148, Oct. 2018, doi: 10.1109/TCC.2016.2545668.

[9] A. D. Watpade, S. Thakor, P. Jain, P. P. Mohapatra, C. R. Vaja, A. Joshi, D. V. Shah, and M. Tariqul Islam, "Comparative analysis of machine learning models for predicting dielectric properties in MoS_2 nanofiller-reinforced epoxy composites," *Ain Shams Eng. J.*, vol. 15, no. 6, Jun. 2024, Art. no. 102754, doi: 10.1016/j.asej.2024.102754.

[10] U. U. Hussine, M. T. Islam, and N. Misran, "Analysis of microstrip patch antenna for L1 and L2 for global positioning system applications," *Jurnal Kejuruteraan (J. Eng.)*, vol. 24, pp. 29–33, 2012.

[11] J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the security of an efficient dynamic auditing protocol in cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 10, pp. 2760–2761, Oct. 2014, doi: 10.1109/TPDS.2013.199.

[12] T. Li, J. Chu, and L. Hu, "CIA: A collaborative integrity auditing scheme for cloud data with multi-replica on multi-cloud storage providers," *IEEE Trans. Parallel Distrib. Syst.*, vol. 34, no. 1, pp. 154–162, Jan. 2023, doi: 10.1109/TPDS.2022.3216614.

[13] P. Jain, H. Chhabra, U. Chauhan, K. Prakash, P. Samant, D. Kumar Singh, M. S. Soliman, and M. Tariqul Islam, "Machine learning techniques for predicting metamaterial microwave absorption performance: A comparison," *IEEE Access*, vol. 11, pp. 128774–128783, 2023, doi: 10.1109/ACCESS.2023.3332731.

[14] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu, and J. Ma, "Data integrity auditing without private key storage for secure cloud storage," *IEEE Trans. Cloud Comput.*, vol. 9, no. 4, pp. 1408–1421, Oct. 2021, doi: 10.1109/TCC.2019.2921553.

[15] J. Wu, Y. Li, T. Wang, and Y. Ding, "CPDA: A confidentiality-preserving deduplication cloud storage with public cloud auditing," *IEEE Access*, vol. 7, pp. 160482–160497, 2019, doi: 10.1109/ACCESS.2019.2950750.

[16] A. Verma, P. Bhattacharya, U. Bodkhe, D. Saraswat, S. Tanwar, and K. Dev, "FedRec: Trusted rank-based recommender scheme for service provisioning in federated cloud environment," *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 33–46, Feb. 2023, doi: 10.1016/j.dcan.2022.06.003.

[17] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Comput. Biol. Med.*, vol. 150, Nov. 2022, Art. no. 106019, doi: 10.1016/j.compbiomed.2022.106019.

[18] Z. Su, Y. Wang, T. H. Luan, N. Zhang, F. Li, T. Chen, and H. Cao, "Secure and efficient federated learning for smart grid with edge-cloud collaboration," *IEEE Trans. Ind. Informat.*, vol. 18, no. 2, pp. 1333–1344, Feb. 2022, doi: 10.1109/TII.2021.3095506.

[19] D. Jatain, V. Singh, and N. Dahiya, "Blockchain base community cluster-federated learning for secure aggregation of healthcare data," *Proc. Comput. Sci.*, vol. 215, pp. 752–762, Jan. 2022, doi: 10.1016/j.procs.2022.12.077.

[20] P. Kumar Sahoo, M. Kumar Panda, U. Panigrahi, G. Panda, P. Jain, M. Shabiul Islam, and M. Tariqul Islam, "An improved VGG-19 network induced enhanced feature pooling for precise moving object detection in complex video scenes," *IEEE Access*, vol. 12, pp. 45847–45864, 2024, doi: 10.1109/ACCESS.2024.3381612.

[21] R. Kumar and R. Goyal, "Performance based risk driven trust (PRTrust): On modeling of secured service sharing in peer-to-peer federated cloud," *Comput. Commun.*, vol. 183, pp. 136–160, Feb. 2022, doi: 10.1016/j.comcom.2021.11.013.

[22] A. Rafique, D. Van Landuyt, and W. Joosen, "PERSIST: Policy-based data management middleware for multi-tenant SaaS leveraging federated cloud storage," *J. Grid Comput.*, vol. 16, no. 2, pp. 165–194, Jun. 2018, doi: 10.1007/s10723-018-9434-6.

[23] O. Malomo, D. Rawat, and M. Garuba, "Security through block vault in a blockchain enabled federated cloud framework," *Appl. Netw. Sci.*, vol. 5, no. 1, p. 16, 2020, doi: 10.1007/s41109-020-00256-4.

[24] A. Hossain, M. T. Islam, T. Rahman, M. E. H. Chowdhury, A. Tahir, S. Kiranyaz, K. Mat, G. K. Beng, and M. S. Soliman, "Brain tumor segmentation and classification from sensor-based portable microwave brain imaging system using lightweight deep learning models," *Biosensors*, vol. 13, no. 3, p. 302, Feb. 2023, doi: 10.3390/bios13030302.

[25] I. Blanquer, F. Brasileiro, A. Brito, A. Calatrava, A. Carvalho, C. Fetzer, F. Figueiredo, R. P. Guimarães, L. Marinho, W. Meira, A. Silva, Á. Alberich-Bayarri, E. Camacho-Ramos, A. Jimenez-Pastor, A. L. L. Ribeiro, B. R. Nascimento, and F. Silva, "Federated and secure cloud services for building medical image classifiers on an intercontinental infrastructure," *Future Gener. Comput. Syst.*, vol. 110, pp. 119–134, Sep. 2020, doi: 10.1016/j.future.2020.04.012.

[26] N. Engheta and R. W. Ziolkowski, *Metamaterials: Physics and Engineering Explorations*. Hoboken, NJ, USA: Wiley, 2006, doi: 10.1002/0471784192.
[27] Z. Yin, Y. Lu, T. Xia, W. Lai, J. Yang, H. Lu, and G. Deng, "Electrically tunable terahertz dual-band metamaterial absorber based on a liquid crystal," *RSC Adv.*, vol. 8, no. 8, pp. 4197–4203, 2018, doi: 10.1039/c7ra13047c.
[28] Y. Villuendas-Rey, J. L. Velázquez-Rodríguez, M. D. Alanis-Tamez, M.-A. Moreno-Ibarra, and C. Yáñez-Márquez, "Mexican axolotl optimization: A novel bioinspired heuristic," *Mathematics*, vol. 9, no. 7, p. 781, Apr. 2021, doi: 10.3390/math9070781.
[29] M. Azizi, U. Aickelin, H. A. Khorshidi, and M. B. Shishehgarkhaneh, "Energy valley optimizer: A novel metaheuristic algorithm for global and engineering optimization," *Sci. Rep.*, vol. 13, no. 1, p. 226, 2023, doi: 10.1038/s41598-022-27344-y.
[30] K. Lee, "Ciphertext outdate attacks on the revocable attribute-based encryption scheme with time encodings," *IEEE Access*, vol. 7, pp. 165122–165126, 2019, doi: 10.1109/ACCESS.2019.2953300.
[31] H. Poostchi and M. Piccardi, "BiLSTM-SSVM: Training the BiLSTM with a structured Hinge loss for named-entity recognition," *IEEE Trans. Big Data*, vol. 8, no. 1, pp. 203–212, Feb. 2022, doi: 10.1109/TBDATA.2019.2938163.
[32] M. Sajjad, Z. Ahmad Khan, A. Ullah, T. Hussain, W. Ullah, M. Young Lee, and S. Wook Baik, "A novel CNN-GRU-Based hybrid approach for short-term residential load forecasting," *IEEE Access*, vol. 8, pp. 143759–143768, 2020, doi: 10.1109/ACCESS.2020.3009537.
[33] M. E. Smid and D. K. Branstad, "Data encryption standard: Past and future," *Proc. IEEE*, vol. 76, no. 5, pp. 550–559, May 1988, doi: 10.1109/5.4441.
[34] M. Masoumi and M. H. Rezayati, "Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 256–265, Feb. 2015, doi: 10.1109/TIFS.2014.2371237.
[35] J.-Y. Lai and C.-T. Huang, "A highly efficient cipher processor for dual-field elliptic curve cryptography," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 56, no. 5, pp. 394–398, May 2009, doi: 10.1109/TCSII.2009.2019327.
[36] Y. Li and G. Wang, "Sand cat swarm optimization based on stochastic variation with elite collaboration," *IEEE Access*, vol. 10, pp. 89989–90003, 2022, doi: 10.1109/ACCESS.2022.3201147.
[37] S. Sugave, B. Jagdale, and D. Rosaci, "Monarch-EWA: Monarch-earthworm-based secure routing protocol in IoT," *Comput. J.*, vol. 63, no. 1, pp. 817–831, Jan. 2020, doi: 10.1093/comjnl/bxz135.

ATUL B. KATHOLE received the B.E., M.B.A., M.Tech., and Ph.D. degrees in computer engineering. He has published more than ten SCI and 30 Scopus articles in different areas now working on the IoT, ML, and security using blockchain and cryptography. He has also received more than 30 lakh sponsorships for his research work from different organizations and countries.

KAPIL NETAJI VHATKAR received the M.Tech. and Ph.D. degrees in computer engineering from VJTI, Mumbai. He is currently an Associate Professor with the Department of Computer Engineering, Pune, Maharashtra, India. His research interests include cloud computing, virtualization, resource elasticity, autonomic computing, and computer networks.

ANKUR GOYAL received the M.Tech. and Ph.D. degrees in computer engineering from Rajasthan Technical University, Kota, India, in 2012 and 2020, respectively. He is currently an Associate Professor with the Department of Engineering and Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India. He has more than 20 years of academic experience. He has designed and conducted various faculty development programs, workshops, and national and international conferences, as a Convener. He has several publications to his credit and has presented 15 research papers with international conferences organized by various central and state universities and government-affiliated engineering colleges. He is guiding two Ph.D. scholars. His areas of research interests include routing protocol, security, blockchain, and image processing. He is a reviewer of various international repute journals.

SHIVKANT KAUSHIK is currently an Associate Professor with the Department of Computer Science and Engineering (AI & DS), Greater Noida Institute of Technology (GNIOT), Greater Noida, Uttar Pradesh, India. He is having an experience of more than 14 years of teaching and supervising students of B.Tech., B.C.A., M.Tech., M.C.A., and Ph.D. in various universities and engineering colleges. He has published numerous research papers in Scopus journals, international and national journals, and conferences. He is supervising M.Tech. and Ph.D. research scholars and many B.Tech. projects. His research interests include digital image processing, image analysis, pattern recognition, the Internet of Things, the Internet of Vehicles, and vehicular ad hoc networks.

AMITA SANJIV MIRGE received the B.E. and M.Tech. degrees in computer engineering. She has published more than two SCI and five Scopus articles in different areas, currently working on the IoT, ML, and security. She has also got more than 2lakh sponsorships for her research work from different organizations and countries.

PRINCE JAIN is currently an Assistant Professor with the Mechatronics Engineering Department, Parul Institute of Technology, Parul University, Vadodara, India. He received the Visvesvaraya Ph.D. Scheme Fellowship to complete the Doctor of Philosophy (Ph.D.) dissertation from Punjab Engineering College (Deemed to be University), Chandigarh, India. He is the author and co-author of about 21 research journal articles, 20 conference papers, and a few book chapters on various topics related to antennas, machine learning, and metamaterials. His research interests include machine learning, artificial intelligence, optimization techniques, metamaterial absorbers/antennas at RF, THz and visible frequencies, material science, nanotechnology, and biomedical signal processing. He is serving as an Academic Editor for *Journal of Electrical and Computer Engineering* (Hindawi) and *PLOS One*. He is serving as a Topical Advisory Panel Member for *Micromachines* and *Materials* (MDPI). He has contributed as a Peer Reviewer of prestigious publishers, including IEEE, Elsevier, IOPscience, Wiley, PIER, Emerald, and PLOS.

MOHAMED S. SOLIMAN (Senior Member, IEEE) received the Ph.D. degree in communications engineering from the Graduate School of Engineering, Osaka University, Japan. He is currently an Associate Professor with the Department of Electrical Engineering, College of Engineering, Taif University, Saudi Arabia. He was granted numerous research projects facilitated by the Deanship of Scientific Research, Taif University. He has authored and co-authored more than 160 articles, which are indexed in Scopus and WOS databases, alongside contributing to five book chapters. He was honored as a Distinguished Researcher, identified among the top one hundred most active researchers, by the Deanship of Scientific Research with Taif University, in 2023. Furthermore, he was honored with the Distinguished Researchers Supporting Project, in 2023, the Scientific Publication Reward, from 2023 to 2024, and the Distinguished Researcher Project as part of the Taif University-Distinguished Scientific Publishing Program and International Appearance (TU-DSPP-2024), administered by the Deanship of Postgraduates and Scientific Research with Taif University. His research interests include wireless communications, phased and timed array signal processing, UWB antennas, MIMO antennas, dielectric resonant antennas, optimization techniques in antenna design, antenna measurement techniques, metamaterial structures, biosensors, RF energy harvesting systems, and numerical methods in electromagnetics. Additionally, he holds the position of a technical program committee (TPC) member of various international conferences. He holds membership in the Microwave Theory and Techniques (MTT) and Antennas and Propagation (AP) Societies. Moreover, he actively contributes to the academic community by serving as a Reviewer of several reputable scientific journals, including PIER Journals (Photonics and Electromagnetics Research Society), *International Journal of RF and Microwave Computer-Aided Engineering* (Wiley-Hindawi Partnership), *Wireless Personal Communications* (Springer), *Electronics*, *Energies* (MDPI), *Automatika: Journal for Control, Measurement, Electronics, Computing and Communications* (Taylor and Francis), and *Measurement* (Elsevier).

MOHAMMAD TARIQUL ISLAM (Senior Member, IEEE) is currently a Professor with the Department of Electrical, Electronic and Systems Engineering, Universiti Kebangsaan Malaysia (UKM), and a Visiting Professor with the Kyushu Institute of Technology, Japan. He is the author and co-author of about 600 research journal articles, nearly 250 conference papers, and a few book chapters on various topics related to antennas, metamaterials, and microwave imaging, with 25 inventory patents filed. Thus far, his publications have been cited 16,600 times and his H-index is 57 (Source: Scopus). His Google scholar citation is 26,000 and H-index is 68. He was a recipient of more than 40 research grants from the Malaysian Ministry of Science, Technology and Innovation, Ministry of Education, UKM research grant, international research grants from Japan, Saudi Arabia and Kuwait. His research interests include communication antenna design, metamaterial, satellite antennas, and microwave imaging. He has been serving as an Executive Committee member for IEEE AP/MTT/EMC Malaysia Chapter, since 2019-2020, the Chartered Professional Engineer (CEng), a fellow of IET, U.K., and a Senior Member of IEICE, Japan. He received several International Gold Medal awards, a Best Invention in Telecommunication Award for his research and innovation, and best researcher awards at UKM. He was a recipient of 2018, 2019, and 2020, IEEE AP/MTT/EMC Malaysia Chapter, Excellent Award. He also won the best innovation award and the Best Researcher award by UKM, in different years. He was a recipient of Publication Award from Malaysian Space Agency, in several years. He has supervised about 50 Ph.D. theses, 30 M.Sc. theses, and has mentored more than 10 postdocs and Visiting scholars. He has developed the Antenna Measurement Laboratory which includes antenna design and measurement facility till 40 GHz. He was an Associate Editor of *IET Electronics Letter*. He also serves as the Guest Editor, *Sensors journal*, Nanomaterials, and an Associate Editor for IEEE Access.