Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Intelligent Edge Healthcare Using Federated Learning and Clustering with Kepler-Optimized Steerable Graph Neural Networks

[1]Rohini. C, [2]Dr. B. Murugeshwari, [3]Dr. A. K. Jaithunbi, [4]Hima Vijayan
[1]*Assistant Professor, Department of Computer Science and Engineering, Velammal Engineering College, Surapet (0009-0001-2589-5918)*
Email: rohini.c@velammal.edu.in
[2]*Professor and Head, Department of Computer Science and Engineering, Velammal Engineering College, Surapet (0009-0003-0734-3348)*
Email: hodcse@velammal.edu.in
[3]*Associate Professor, Department of Computer Science and Engineering, R. M. D. Engineering College, Kavaraipettai (0000-0002-3112-4909)*
Email: akj.cse@rmd.ac.in
[4]*Assistant Professor, Information Technology Department, S.A. Engineering College, Chennai (0009-0001-3862-6020)*
Email: himavijayan@saec.ac.in

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Nowadays, people frequently use smart healthcare systems (SHS) to use a variety of smart devices to monitor their health. The SHS uses Internet of Things (IoT) and cloud infrastructure for data collection, transmission via smart devices, data processing, storage, and medical advice. It can be difficult to process so much data from so many IoT devices in a short period. Therefore, in SHS, technical frameworks like fog computing or edge computing can be utilized as mediators between the user and the cloud. It shortens response times for lower-level (edge-level) data processing. If anomalous data is generated, it will react quickly and securely to store and retrieve important data. This paper presents a smart health monitoring system architecture comprising three core layers: Data Generation, Edge Computing, and Cloud Storage. The Data Generation Layer utilizes IoMT devices, wearables, and sensors connected to an Edge-IoT Gateway for stream data acquisition. The Edge Computing Layer uses Z-score Min-Max normalization-based preprocessing, cascading residual graph convolutional networks to extract features, and the Steerable Graph Neural Network with Kepler Optimization Algorithm (SGNN-KOA) to improve the performance. The Cloud Storage Layer is provided to enhance the security feature of the cloud network using lightweight dynamic elliptic curve cryptography with Schoof's algorithm for data deposit. As mentioned, the system is designed to support multi-modal learning, adaptive feedback, and secure access for facility comprehensive health management. With an accuracy rate of over 99%, convergence in fewer iterations, and high classification capabilities using measures like AUC of 0.99, the suggested method outperforms the others in terms of accuracy at epochs, reduced divergence, and improved accuracy.

Keywords: Cloud Storage, Data Security And Privacy, Edge Computing, Kepler Optimization Algorithm, Smart Healthcare Systems, Steerable Graph Neural Network.

1. INTRODUCTION

One of a living being's basic needs is health. A nation's effective healthcare system is a key indicator of its level of development. India is the second most populous country around the globe. Providing a high-quality, consistent health care service is difficult due to the nation's large population and wide range of living situations [1-2]. SHS were created as a result of the healthcare industry's digital revolution. With the aid of numerous technologies and smart gadgets, SHS provides services to the public. SHS's technological development phases have progressed from the healthcare framework's version 1.0 to 4.0 [3-4].

The expansion of the IoT makes it possible for intelligent healthcare systems to intervene on behalf of patients who are unable to do so in emergency scenarios, such as environmental assisted living (AAL) and pandemics. In this case, an SHS collects patients' immediate physiological records via an Internet of Things network at any time and from

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

any location, providing intelligent purposes for early-stage detection, real-time health monitoring, and making decisions with cognitive abilities [5-6]. Because of this, there is a growing need for IoT systems, which are expected to be worth $158 billion by 2022. Furthermore, this industry's hyper-growth has been pushed by the current COVID-19 outbreak [7-9].

Smart gadgets that are connected to a network generate vast amounts of data, which are then analyzed to provide better patient suggestions and support the healthcare system as a whole. However, as this data includes a medical history and indicates patient behavior, it needs proper protection and privacy guarantees [10-12]. Any health-related information that is pertinent to making decisions on an individual's health is referred to as healthcare data in this context.

The information gathered can be applied to self-care, health promotion, prevention, treatment, and cure, as well as broader public health initiatives [13-14]. This information can influence treatment plans, give insight into a person's well-being, and aid in the investigation of new disease trends and the adjustment of treatment approaches.

Novelty and Contribution

- The proposed method incorporates a multi-layer architecture that effectively blends secure cloud storage, edge computing, and real-time data collection for all-encompassing smart health monitoring.
- Through the use of advanced preprocessing techniques, including Z-score Min-Max normalization and feature extraction using cascading residual graph convolutional networks, the proposed method enhances the accuracy and robustness of health data analysis.
- To enhance performance and enable accurate and scalable medical condition prediction and anomaly detection, a steerable graph neural network optimized with the Kepler method is presented.
- The system incorporates dynamic elliptic curve cryptography with Schoof's algorithm for lightweight yet strong encryption, ensuring data privacy and security throughout the entire healthcare ecosystem.
- Through multi-modal learning and adaptive feedback mechanisms, the framework continuously improves predictive models based on individual health trends, offering proactive and customized healthcare treatments.

The outstanding of this Section 2 examines the literature, Section 3 suggests methods, Section 4 displays the findings and discussion, and Section 5 provides the conclusion.

2. LITERATURE SURVEY

In 2023 Lai et al. [15] have introduced the EICPP, an innovative, cooperative, and private privacy protection system for smart medicine. That secures patient privacy and guarantees model correctness by combining federated learning with edge computing. In addition to supporting auxiliary diagnostics and health monitoring, the KubeFL architecture boasts a very accurate federated learning training approach. The suggested method's limited scalability in edge environments with limited resources is a downside.

Wang et al. (2022) [16] have presented the protection of privacy framework for edge computing-based federated learning (PPFLEC). To solve privacy and security issues in edge computing settings such as smart healthcare. In contrast to homomorphic encryption, the technique employs a lightweight system for protecting privacy based on a weight mask and shared secret, which is more precise and effective. The method is built to withstand replay assaults and preserve message integrity. The suggested method's disadvantage is that it can be more difficult to adopt and maintain.

Singh and Chatterjee (2023) [17] have offered a secure framework for Edge of Things (SEoT)-based monitoring of health in real time that preserves data security and privacy. Clustering techniques for abnormality identification and encryption based on attributes for safe access are also included in the framework. The findings of the experiment demonstrate enhanced performance with great accuracy. Potential scaling issues with real-time processing are the suggested method's disadvantage.

In 2023 Wang et al. [18] have introduced the FRESH framework, which is according to the defense of ring signature and FL for exchanging physiological data. It trains machine learning models by uploading model parameters to a

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

central server via edge computing devices. FRESH is appropriate for extensive intelligent systems of healthcare with FL involving several users because it lowers SIA success rates and increases the effectiveness of verifying signatures. For edge devices, the suggested method's disadvantage is an increase in processing overhead.

2.1 Problem Statement

The existing smart health monitoring systems face significant challenges in collecting real-time data, protecting privacy, and processing data efficiently. Many systems rely on traditional methods of data processing, which are not capable of handling large volumes of data generated by IoMT devices and wearables. Moreover, securing sensitive health data in cloud storage while providing low latency is another serious issue. Current models lack scalability and adaptability and therefore are unable to offer health insights at an individual level. The proposed method will fill the gaps by introducing multi-layer architecture with edge computing to collect and process real-time data. The lightweight dynamic elliptic curve cryptography and Schoof's algorithm have been used to improve data security. The use of a steerable graph neural network optimized with Kepler's algorithm ensures high-performance health data analysis. Moreover, the system supports scalable, multi-modal learning for adaptive, personalized healthcare solutions, which improves the protection of privacy and offers efficient analytics in smart health environments.

3. PROPOSED METHODOLOGY

Figure 1 illustrates a comprehensive smart health monitoring system's architecture, featuring three core layers: Data generation at the edge, edge computing, and cloud storage are the key areas of focus. This layer comprises data sensors, IoMT devices, and wearables on a human body connected to an edge-IoT gateway that realizes real-time health data generation. The edge computing layer is responsible for data gathering, Z-score Min-Max normalization-based preprocessing, cascading residual graph convolutional networks for extracting features from the data, and a steerable graph neural network that uses the Kepler algorithm to improve its performance. The cloud storage layer also guarantees effective storage and the application of lightweight dynamic elliptic curve cryptography together with Schoof's algorithm to enhance secure data storage. Furthermore, the system includes a flexible, multi-modal learning architecture for the prediction and early diagnosis of health status. It uses tunable feedback processes to update the models according to the client's health characteristics. The access and authentication layer provides end-to-end, integrated, and complete healthcare assistance by providing a privacy-preserving connection for community health management, doctors, nurses, remote monitoring, laboratory technicians, and clinics.

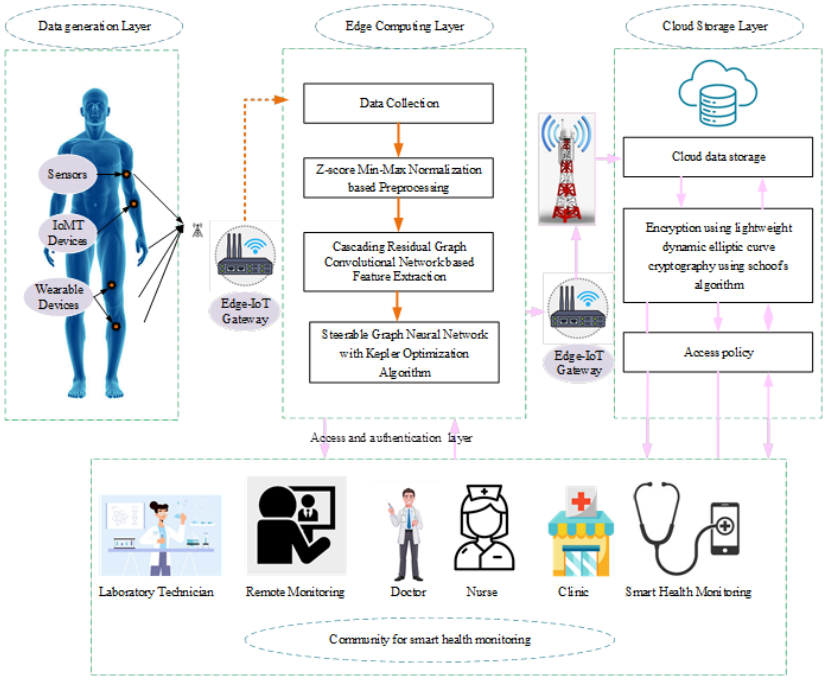

Figure 1: Illustration of the proposed method

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.1 Dataset

The proposed method utilizes the MHEALTH dataset, obtained from the UCI Machine Learning Repository, that targets analysis of physical activities and vital signs using multimodal body sensing. Data inputs are passed on to the preprocessing stage.

3.2 Z-score Min-Max Normalization based Preprocessing

Preprocessing using the Z-score min-max normalization is applied to the input data. Privacy-preserving healthcare in edge computing, where data preprocessing includes the application of the Z-score Min-Max normalization. This approach seeks to improve the quality of health data by establishing health data standards, delivering the right healthcare statistics analysis, and taking care of rigorous health data privacy. The issue of outliers is addressed by the statistics normalization technique called Z-score normalization. The median and standard deviations pertaining to the characteristic under investigation are used to convert the characteristic data [19]. In particular, values for the characteristic under study are converted using the following equation into acceptable normalized values.

$$\kappa' = \frac{\kappa' - \eta}{\delta} \tag{1}$$

Where δ stands for the characteristics' standard deviation, while η is the selected characteristic's median value. When the Z-score normalization approach is used, numbers exactly equal to the median are placed at zero, amounts below average appear as negative numerals, and scores are displayed as positive scores above the median.

Min-max normalization is a widely used technique for normalizing data that entails transforming the characteristic's values into new, smaller values that lie within a predetermined range, usually [0–1]. It is known that any correlation in the data under study is preserved by min-max normalization. In the characteristic under study, the following equation is used to transfer the values to a new standardized value.

$$\kappa' = \frac{\kappa - Min_p}{Max_p - Min_p}\left(New\_Max_p - New\_Min_p\right) + New\_Max_p \tag{2}$$

Where Max_p denotes the highest value for the given attribute p, Min_p is the minimum value for the given attribute p, κ is the original value for the provided feature, New_Max_x and New_Min_p are the maximum and minimum values for the new evaluated range, and v' is the new normalized value. Next, the preprocessed data is subjected to the feature extraction technique.

3.3 Cascading Residual Graph Convolutional Network based Feature Extraction (CRGCN)

Extracting features is used to extract the significant elements from the preprocessed data. The CRGCN performs feature extraction of multi-modal healthcare data from different patients under the protection of user privacy in smart healthcare systems relying on edge computing environments. The CRGCN is intended to efficiently learn and extract valuable features from complex health care data while protecting patient privacy. The technique ensures effective calculations of the heterogeneous medical data on edge devices since it identifies residual connections and graph convolutional networks [20-21]. The framework improves model performance, and guarantees privacy protection of patients' information through privacy-preserving methodologies for the secure and scalable deployment of healthcare applications.

Embedding Initialization

To initialize the embedding of samples and features, let $G \in R^{A \times v}$ and $U \in R^{B \times v}$ be the integrating matrices. The integrating size A is denoted by v, while the number of samples and features is denoted by B. Using the one-hot integrating matrix NM^S and NM^D for samples and features, the embeddings are formally initialized as follows:

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

$$f_s^0 = G.NM_s^S, \qquad f_d^0 = U.NM_d^D, \tag{3}$$

The initialized sample s 's and features d 's embeddings are denoted by f_s^0 and f_d^0, respectively. The sample s 's (features d 's) one-hot vector is $NM_s^S\left(NM_d^D\right)$. Additionally, the only learnable parameters are the embedding matrices G and U.

Residual block cascade

Cascaded residual blocks are used in the suggested approach. Learning and creating feature embeddings using region-based features, pixel intensity, or fundamental data improves accuracy. To improve the accuracy of the suggested approach, features are generated from past interaction data using neighborhood aggregation and graph-structured data.

$$f_s^{(k)} = agg\left(\left\{f_p^{(k-1)} : p \in B_s\right\}\right) \tag{4}$$

The feature embedding of the sample s 's neighboring node from the $(k-1)-th$ layer is shown by $f_p^{(k-1)}$, whereas agg represents the function of aggregation, which aggregates the data from the sample's neighboring nodes. Here, the feature embedding in the $k-th$ layer is shown by $f_s^{(k)}$.

By integrating derived data patterns and maintaining previous knowledge through residual connections, the suggested method offers enhanced feature extraction. After extracting data using summation and L2 normalization to balance the data, each block is calculated as the total of the characteristics from the block before it. By combining interdependencies across the data patterns for improved categorization, this technique enhances feature learning.

$$\tilde{f}_s = \frac{f_s'}{\left\| f_s' \right\|_2}, \qquad \tilde{f}_f = \frac{f_d'}{\left\| f_d' \right\|_2} \tag{5}$$

Combine the characteristics acquired in the current block utilizing the residual link after normalization with the sole output from the previous block.

$$f_{s_{Out}} = f_{s_{In}} + \tilde{f}_s,$$
$$f_{d_{Out}} = f_{d_{In}} + \tilde{f}_d, \tag{6}$$

In the current block, the input sample and feature embeddings are represented by variables $f_{s_{In}}$ and $f_{d_{In}}$. These variables also serve as the block's output. The symbols $f_{s_{Out}}$ and $f_{d_{Out}}$ stand for the output sample and feature embedding of the present moment block, respectively. The framework enhances model performance and ensures patient data privacy protection using privacy-preserving techniques for the safe and scalable implementation of medical applications.After that, the extracted features are subjected to categorization.

3.4 Steerable Graph Neural Network with Kepler Optimization Algorithm (SGNN-KOA)

After feature extraction, prediction occurs. The Steerable Graph Neural Network (SGNN) along with the Kepler Optimization Algorithm (KOA) to formulate smart healthcare systems that provide accurate and enhanced health data analysis. The method relies on the SGNN's capability to encode intricate relations in the multimodal data; Kepler optimization further enhances the network for performance optimization, health condition prediction, and anomaly detection compliance, which is adaptive, accurate, and commensurate with the requirements for scalable healthcare

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

applications [22]. The input data is $H=\{h_p\}_{p=1}^{H}\in R^k$, where each point's feature dimension is $k\geq 3$. A Gaussian kernel is then used to weight each edge: Considering $p=1,\ldots H,$

$$U_{p,q}=\begin{cases}Exp\left(-\left\|h_p-h_q\right\|^2/\eta^2\right) If\ q\in \mathrm{NN}_m(p)\\ 0 \qquad\qquad Otherwise\end{cases} \tag{7}$$

The set of m neighbors anchored at h_p is represented by $NN_m(p)=\{q:(p,q)\in U\}\cup\{p\}$ (including itself), and η is the Euclidean distance mean $\left\|h_p-h_q\right\|, q\in \mathrm{NN}_m(p)$. Therefore, a multimodal data set is represented as a tuple $C=(V,U)$, where U is the weight adjacent matrix and $V=\{1,2,.....N\}$ is the multimodal data vertex set.

Steady graph analysis of random walks (RW) employs sub-graph sampling techniques called fields. Breadth-first sampling (BFS) and depth-first sampling (DFS) are the two algorithm types that are included in this category. The complete utilization of nearest-neighbor features is supported by BFS, whereas DFS encourages remote exploration. Begin with $g_0=\rho$ and use g_p to represent the $p-th$ vertex in the RW. Vertex g_p is produced by the distribution that follows:

$$U\left(g_p=a\middle|g_{p-1}=\rho\right)=\begin{cases}\pi_{\rho,a} & If\ (\rho,a)\in U\\ 0 & Otherwise\end{cases} \tag{8}$$

Where the normalized transition probabilities between vertices ρ and a is $\pi_{\rho,a}=K^{-1}U_{\rho,a}$ which is obtained by weighting the matrix of adjacency with degree matrix K.

The procedure now assesses the transition probabilities $\pi_{\rho,a}$ on edges (ρ,a) leading from v to determine the next vertex, g_{p+1}. The transition probability was set using the formula $\pi_{\rho,a}=\beta_{ho}(f,a)\cdot U_{\rho,a}$, where

$$\beta_{ho}(f,a)=\begin{cases}1/h & If\ e_{f,a}=0\\ 1 & If\ e_{f,a}=1\\ 1/o & If\ e_{f,a}=2\end{cases} \tag{9}$$

and the counting amount of hops between points f and a is indicated by $e_{f,a}$. Keep in mind that $e_{f,a}$ must be between {0, 1, and 2}. In other words, the method has a $1/h$ chance of folding back to the original node f, a $1/o$ chance of exploring outward, and a $1/h$ chance of traversing to another sibling node that is directly connected to f. The accuracy and scalability of health condition prediction and anomaly detection are significantly improved by this method, which efficiently models intricate relationships in multimodal data and enhances network performance. For real-time health monitoring, the SGNN architecture offers a reliable, flexible approach that guarantees more accurate and individualized medical results. The error rate of the neural network is maximized by optimizing the identified data.

3.4.1 Kepler Optimization Algorithm (KOA)

The suggested approach was inspired by Kepler's optimization algorithms (KOA) of planet-wide motion. In hypothetical elliptical orbits, the sun and planets represent the search space. The method can more efficiently explore

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and use the search space by taking into account several factors, including item position, mass, attraction force, and velocity [23]. The KOA is used to minimize the error rate of the proposed method.

$$Fitness\ Function = Min(MSE) \tag{10}$$

Following the steerable graph neural network with the Kepler optimization algorithm follows data encryption. This enables the system to protect sensitive health data from unauthorized access while it is being transferred or processed. Data privacy is achieved using lightweight encryption techniques like elliptic curve cryptography in combination with Schoof's algorithm to avoid overloading computational processes. This approach is highly beneficial because it achieves both security and high degrees of computation while preserving the confidentiality of health data in real-time health analysis systems.

3.5 Encryption using lightweight dynamic elliptic curve cryptography using schoof's algorithm

Ensuring secure encryption of sensitive health data in real-time healthcare systems by combining lightweight dynamic elliptic curve cryptography with Schoof's algorithm strikes a balance between robust privacy protection as well as minimal computational overhead for processing efficiency.

- **Elliptic curve cryptography**

One kind of public-key encryption system is elliptic curve cryptography. Elliptic curves can be applied to digital signatures and key exchange. The fundamental steps involved in implementing ECC are as follows. To implement the Elliptical Curve Cryptography, the publicly known entities such as equation constants a, b, p, equation group and the generator or base point G are essential for the equation. Here Alice and Bob created a public and private key. The condition for the public and private key generation is given in Eqn. (11), (12)

$$public\_key \in [1, p-1] \tag{11}$$

$$public\_key = private\_key * G \tag{12}$$

A key agreement mechanism called the Elliptic Curve based Diffie-Hellman (EC-DH) Key exchange is employed to exchange a public and private keys between two parties. The only operation that separates EC-DH from the standard Diffie-Hellman Key Exchange (DHKE) is that EC-DH uses Elliptic Curve Point Scalar Multiplication rather than exponentiations in modules. The key sharing between Alice and Bob is explained in Eqn. (13) and (14)

$$Alice\, compute\, K_A(K_B * G) \tag{13}$$

$$Bob\, compute\, K_B(K_A * G) \tag{14}$$

Here K_A represents the private key of Alice, and K_B indicates the private key of Bob. Both the keys are keys are similar; therefore, the final shared key is in form of $K_B * K_A * G$. An encoded point on the curve represents the message in this cryptosystem. Let us assume that point is P_M . A point with the following coordinates in Eqn. (15) is the cipher.

$$cipher = \{K_A G, (P_M + K_A * \tilde{K}_B)\} \tag{15}$$

Here K_A is the Alice's private key and $\tilde{K}_B$ indicates the Bob's public key. To compute the variable yC_m at Bob enter $(P_M + K_A * K_B * G)$ where $K_A * G$ equal to xC_m . Hence decryption process is carried out as given in Eqn. (16).

$$P_M = yC_m - K_B xC_m \tag{16}$$

- **Schoof's algorithm**

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The least preferred method was used in the beginning stages of elliptic curves to count the total amount of points [17], which was done naively. This iterates over all of the finite field's elements over p while maintaining track of the number of items that fulfil the equation for the elliptic curve. This strategy is not practical for devices with limited resources on a wider scale due to its high time complexity, which could lead to failure and restrict its intended use.

Schoof's algorithm is the very first time-based polynomial technique to count the locations of points on an ellipse curve EC_p. With little resources, this method is quite quick and doable. Its space complexity is specified as $O(n^3)$ and its time complexity is denoted as $O(n^{5+O(1)})$ where $n = \log p$. This method takes advantage of Hasse's Theorem, which gives a range of finite possible values for the elliptic curve EC_p. With p being the prime number and t being the trace of Frobenius modulo of numerous tiny primes l, this method describes $EC_p = p+1-t$. The Chinese Remainder Theorem is used to find the Frobenius trace. The Schoof's Algorithm was enhanced resulting in a time complexity of $O(n^{4+O(1)})$ and a space complexity of $O(n^3 \log n)$. To model the dynamic behaviour of the ECC following step are considered.

- **Randomising the constants**

Three constants $a, b \, and \, p$ make up the elliptic curve equation $y^2 = x^3 + ax + b$. Here a is the x-coefficient, b is the equation's constant, and p is the prime number that the field is generated over. The method can create an elliptic curve over a limited area and produce random integers a, bp with the aid of the pseudo randomized number generator (PRNG). In order to prevent the curve from becoming singular—that is, to prevent the discriminant from equal to zero—the constants a and b are produced. A smaller bit length a, bp can be constructed to randomize the equations' coefficients and create an entirely novel elliptic curve at each execution on a machine with limited resources and absence of technical standards.

- **Counting the Points of Elliptic Curve**

Counting a certain amount of points is one challenge in creating an elliptic curve. To improve the reliability of the dynamic elliptic curve cryptography model, the number of spots on the curve must be prime number since elliptic curves containing prime orders n are thought to be difficult to solve. Furthermore, the Discrete Logarithm problem (DLP) is challenging to answer if n is a prime number. Now, the sequence of the curve is calculated using Schoof's Algorithm, and it is verified that the created elliptic curve has a prime order to ensure that it is safe for usage.

- **Randomly choosing the generator point**

Every additional point on the curve is generated from the generator point. Choosing the appropriate base point is crucial for creating a safe elliptic curve in cryptography. Every point on the elliptical arc is a generator point if the cofactor variable h of the curve equals 1. The entire group is chosen as one cyclic group in order to select a secure curve with $h \leq 4 \text{and}$ h equal to 1. The sequence of any single point is proportional to the overall amount of pointers on the curves. In this case, the relation is $EC_p = nh$. The steps below should be followed in order to choose a starting point for the line with $h > 1$.

- Choose a point Z at random on the curve EC_p.
- Check $hZ = O_\infty$ if not, choose the point once more.
- Check if $nZ = O_\infty$ now; if not, proceed to the very initial step.
- With order n, provide Q as the starting point.

Generator points are crucial components of the elliptic curve encryption system and serve as the basis for the ECC's ECDLP issue. Therefore, it needs to be chosen with care. From a security perspective, the order should have a big

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

prime number and a cofactor of one. The secp256k1 curve, which is used to represent the "Bitcoin" curve, has an order of a huge prime number and a cofactor of 1.

The polynomial-time point-counting method on the curve is Schoof's algorithm. The Schoof's algorithm is implemented by Sage Math. Resilient elliptic curves are those having a prime number of points. Cofactor will equal 1 because the elliptic curve belongs to a prime order group, denoted by h. Consequently, the method may deduce that $EC_p = n$ and that any spot on the graph will serve as a generator point using the equation $EC_p = nh$. To produce all the additional points on the arc, choose a generator spot at randomness. User-produced bit-length constants for IoT-like devices can be reduced. Although the key length will be shorter with a smaller bit length, the computation time will be faster. Additionally, the generated elliptic curve is only used once. For the produced curve, a pair of public and private keys can be generated. The private key for cryptography can be defined as an arbitrary number selected from $[1, p-1]$.It is also possible to produce an n-bit private key by setting the upper bound to $p-1$ and the lower bound to the lowest n-bit value. The scalar generated by the private key and Base Point, G, is known as the public key. The public key will be located on the curve as each point on the curves is a double of G. Using the recently developed cryptosystem, information can be encoded, decrypted, and verified. This approach depends on the pseudorandom number generator (PRNG) and the bit length of the prime integer. Therefore, a bigger bit-length integer and a secure PRNG ought to be employed for a secure cryptosystem.

The proposed method outlines a smart health monitoring system with three core layers: data generation at the edge, edge computing, and cloud storage. The system uses sensors, IoMT devices, and wearables for real-time health data generation. The Edge Computing layer gathers data, while the Cloud Storage layer ensures secure storage. The system also features a flexible learning architecture for early health diagnosis.

4. RESULTS AND DISCUSSION

The results and discussion section, which offers a thorough comparative performance comparison between the proposed approach and existing methods, demonstrates the methodology's effectiveness. The suggested approach is implemented in Python, enabling flexible experimentation and fine-tuning.

4.1 Dataset Description

The MHEALTH Dataset was obtained for the experiment from the UCI Machine Learning Repository. There are 121,781 web hits, 23 attributes, and 120 instances in the dataset. This dataset, which includes the vital signs and body movements of ten volunteers engaging in a variety of physical activities, is based on multimodal body sensing. The dataset measures 24 body sensing parameters through 12 activities gathered from three sensor devices. Important body parameters have been measured by implanting Shimmer3 wearable sensors on the subject's left ankle, right wrist, and chest. The implanted sensor in the chest, which tracks arrhythmias and fundamental cardiac parameters, can be used to obtain 2-lead ECG readings. Every volunteer's (subject's) data is kept in a separate log file. The various sample values (by rows) for each of the 24 body traits (attributes) detected by the three sensors positioned on the human body (by columns) are contained in each log file.

4.2 Performance comparison with existing methods

This section evaluates the suggested strategy's effectiveness against a number of existing methods. The proposed methodology has been contrasted with other current methods, such as EICPP [15], PPFLEC [16], SEoT [17], and ML [18]. The comparison uses F1 score, specificity, recall, accuracy, and precision as key performance metrics to show how well the proposed method performs in recognition.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

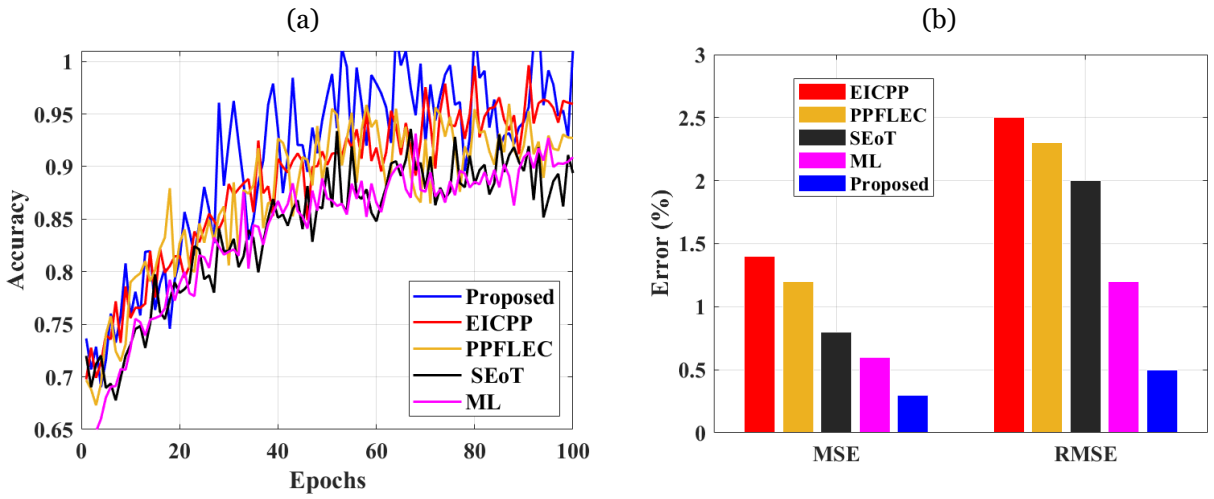

Figure 2: Performance and Error Metrics Comparison for Various Methods: (a) Accuracy over Epochs and (b) Error Metrics Comparison

Figure 2 shows the performance and error metrics comparison for various methods: (a) accuracy over epochs and (b) error metrics comparison. The accuracy of each epoch is displayed in Figure2 (a), and it is clear that the suggested approach has the highest accuracy episode and converges more quickly than the other methods. While PPFLEC continuously rises but still lags behind, EICPP maintains relatively stable overall and stays near the reference line. SEoT shows moderate accuracy with distinct oscillations, while the worst results belong to ML with the slowest accuracy increase. Each of the methods reveals increased accuracy over time, rising and then flattening, while the proposed method is both more resistant and efficient. In Figure 2 (b) comparing the MSE and RMSE percentages for five methods: EICPP, PPFLEC, SEoT, ML, and Proposed. The proposed method represents the lowest error percentages for both MSE and RMSE, which highlights the best performance. Accordingly, PPFLEC has the second-highest RMSE values based on both errors, whereas EICPP has the largest. In terms of errors, SEoT and ML have values in between, while the bars under Proposed illustrate the method's efficiency.

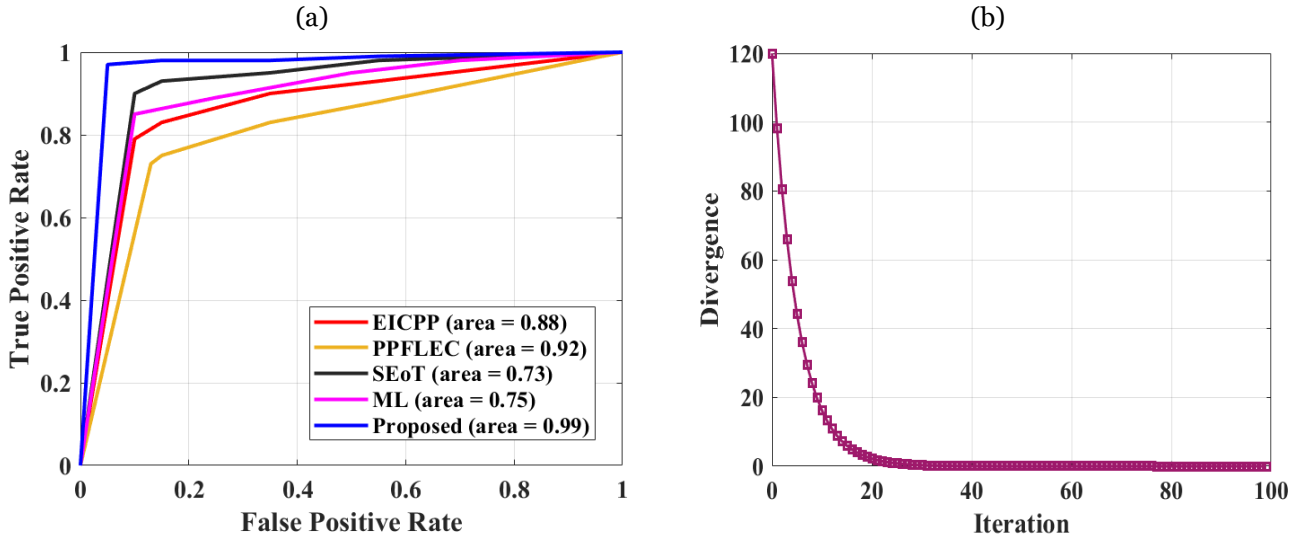

Figure 3: (a) ROC Curve Comparison of Methods with AUC Scores and (b) Divergence Convergence over Iterations

Figure 3 (a) illustrates the ROC that shows the rate of true positive against the rate of false positive of different methods. The accuracy of the proposed method is thus the highest and is further verified by the Area under the Curve (AUC = 0.99), which shows the model's aptness in class distinction. PPFLEC comes next with an AUC of 0.92, which

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

is rather high accuracy but still somewhat lower than the first three methods. EICPP yields a rather high AUC of 0.88, whereas both ML and SEoT perform significantly worse with AUCs of 0.75 and 0.73, respectively. The proposed method provides the most reliable classification capability and is better in comparison with other methods. The deviation of the divergence values after 100 iterations is shown in Figure 3 (b), where they converge to a somewhat higher value. This measure rapidly drops from a value of roughly 120 during the first 20 repetitions, suggesting a high optimality or learning rate. After 20 iterations, the values approach zero as the limit approaches the solution, and the iterations then oscillate around a very tiny number, suggesting that the system has almost reached an ideal solution. The fast convergence that was followed by oscillations confirms the strategy's advantage and consistency in providing a relatively fast convergence while maintaining precision throughout the optimization process.

Table 1: Performance Comparison of Existing Methods and the Proposed SGNN-KOA

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Error rate	Computational Time (s)
EICPP [8]	85.78	86.22	87.1	86.65	1.05	2.78
PPFLEC [9]	88.92	89.11	89.67	89.39	1.12	3.1
SEoT [10]	89.34	89.87	89.22	89.54	1.07	2.95
ML [11]	90.65	90.5	90.22	90.36	1.01	3.25
Proposed SGNN-KOA	99.85	99.62	99.71	99.65	0.01	0.02

The table compares the performance of four existing methods, EICPP, PPFLEC, SEoT, and ML, with the proposed SGNN-KOA over various metrics. The proposed method outperforms all existing methods with more than 99.50% F1 score, recall, accuracy, and precision and with a significantly low error rate of 0.01%. In contrast, the existing methods exhibit accuracy ranging from 85.78% to 90.65%, with error rates above 1.01%. The proposed method also has a more rapid computational time, at approximately 0.02 seconds, whereas the existing methods all take more than 2.67 seconds.

5. CONCLUSION

The proposed SGNN-KOA (Steerable Graph Neural Network with Kepler Optimization Algorithm) significantly improves the performance and efficiency of smart healthcare systems. It reaches over 99.50% in F1 score, recall, accuracy, and precision, surpassing the existing methods (EICPP, PPFLEC, SEoT, ML), which range from 85.78% to 90.65%. SGNN-KOA also shows an error rate of 0.01%, whereas existing methods have over 1.01% and take data processing time of 0.02 seconds. The proposed method is much faster than other methods, which take over 2.67 seconds. This method will ensure high performance, low error rates, and fast processing and thus can be used in real-time healthcare applications with privacy-preserving techniques to handle sensitive health data. Future work will expand the proposed SGNN-KOA framework by incorporating more sensors and multimodal data sources in order to make it more accurate for health condition prediction. More advanced privacy-preserving techniques, like federated learning, may also be integrated to improve security without compromising model performance. Scalability of the model will be tested for large datasets and diverse healthcare settings with a focus on adaptation to different populations and conditions.

REFERENCES:

[1] Cao, W., Shen, W., Zhang, Z. and Qin, J., 2023. Privacy-preserving healthcare monitoring for IoT devices under edge computing. *Computers & Security*, *134*, p.103464.

[2] Dr. M. Preetha, Dr. Padmavathy E, K. Murugesan, R. Ashok Kumar and Vidhya Muthulakshmi R (2024), “Contextual Attention Greylag Goose Neural Networks Based Efficient Energy Consumption and Fault Tolerant Method for Clustering and Reliable Routing in Wireless Sensor Network”, Library Progress International, Vol.44 No.3, Jul-Dec 2024: P.12708-12718, ISSN 0970 1052.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[3] M. Preetha, Raja Rao Budaraju, Jackulin. C, P. S. G. Aruna Sri, T. Padmapriya "Deep Learning-Driven Real-Time Multimodal Healthcare Data Synthesis", International Journal of Intelligent Systems and Applications in Engineering (IJISAE), ISSN:2147-6799, Vol.12, Issue 5, page No:360-369, 2024.

[4] Nasser, N., Emad-ul-Haq, Q., Imran, M., Ali, A., Razzak, I. and Al-Helali, A., 2023. A smart healthcare framework for detection and monitoring of COVID-19 using IoT and cloud computing. *Neural Computing and Applications*, pp.1-15.

[5] S. Srinivasan, S. Sajini, Balaji Singaram, K. Saravanan, K. B. Kishore Mohan," Deep Graph Neural Networks for Multi-Image Super Resolution Reconstruction," International Journal of intelligent systems and applications in engineering, vol. 12, no.15s, p.158-164, 2024.

[6] Gupta, P., Chouhan, A.V., Wajeed, M.A., Tiwari, S., Bist, A.S. and Puri, S.C., 2023. Prediction of health monitoring with deep learning using edge computing. *Measurement: Sensors*, *25*, p.100604.

[7] Humayun, M., Alsirhani, A., Alserhani, F., Shaheen, M. and Alwakid, G., 2024. Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency. *Journal of Cloud Computing*, *13*(1), p.37.

[8] Dr. A Bamila Virgin Louis, Dr. M. S. Maharajan, V. Vaithianathan, S. Balaguru, Dr. P. Bhuvaneswari and Dr. M. Preetha (2024), "Graph Fick's Neural Networks for Traffic Prediction and Resource Allocation in 6G Wireless Systems", Library Progress International, Vol.44 No. 3, Jul-Dec 2024: P.13412-13422, ISSN 0970 1052.

[9] Khanh, Q.V., Hoai, N.V., Van, A.D. and Minh, Q.N., 2023. An integrating computing framework based on edge-fog-cloud for internet of healthcare things applications. *Internet of Things*, *23*, p.100907.

[10] Datta, S. and Namasudra, S., 2024. Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile edge computing. *IEEE Transactions on Consumer Electronics*.

[11] Dr. J. Venkatesh, M. Mutharasu, Charumathi A C, Dr. M. S. Maharajan, Neelamegam Devarasu and Dr. M. Preetha (2024), "IOT-Based Smart Health Care Patient Monitoring System Using Dual Sampling Dilated Pre-Activation Simplicial Convolution Neural Network with Artificial Hummingbird Algorithm", Library Progress International, Vol.44 No. 3, Jul-Dec 2024: P. 14750-14760, ISSN 0970 1052.

[12] M. Sughasiny, K.K.Thyagarajan, A. Karthikeyan, K. Sangeetha, K Sivakumar, "A Comparative Analysis of GOA (Grasshopper Optimization Algorithm) Adversarial Deep Belief Neural Network for Renal Cell Carcinoma: Kidney Cancer Detection & Classification," International Journal of Intelligent Systems and Applications In Engineering, ISSN: 2147-6799, 2024, 12(9s), 43–48.

[13] Balaji Singaram, Lakshmi. B, Dr.M.Preetha, V.K. RamyaBharathi, Dr.S.Muthumarilakshmi, Rakesh Kumar Giri "A Smart IoT-Based Fire Detection and Machine Learning Based Control System for Advancing Fire Safety" Nanotechnology Perceptions, ISSN 1660-6795 2024, Vol: 20, 5s, 229-244.

[14] Dr.M.Preetha, Balaji Singaram, Dr.I. Manju, B.Hemalatha, P. Bhuvaneswari "Machine Learning in Breast Cancer Treatment for Enhanced Outcomes with Regional Inductive Moderate Hyperthermia and Neoadjuvant Chemotherapy" Nanotechnology Perceptions, ISSN 1660-6795 2024, Vol: 20, 5s, 245-259.

[15] Lai, J., Song, X., Wang, R. and Li, X., 2023. Edge intelligent collaborative privacy protection solution for smart medical. *Cyber Security and Applications*, *1*, p.100010.

[16] Wang, R., Lai, J., Zhang, Z., Li, X., Vijayakumar, P. and Karuppiah, M., 2022. Privacy-preserving federated learning for internet of medical things under edge computing. *IEEE journal of biomedical and health informatics*, *27*(2), pp.854-865.

[17] Singh, A. and Chatterjee, K., 2023. Edge computing based secure health monitoring framework for electronic healthcare system. *Cluster Computing*, *26*(2), pp.1205-1220.

[18] Wang, W., Li, X., Qiu, X., Zhang, X., Brusic, V. and Zhao, J., 2023. A privacy preserving framework for federated learning in smart healthcare systems. *Information Processing & Management*, *60*(1), p.103167.

[19] S. Srinivasan, D. Deva Hema, Balaji Singaram, D. Praveena, K. B. Kishore Mohan, M. Preetha," Decision Support System based on Industry 5.0 in Artificial Intelligence," International Journal of intelligent systems and applications in engineering, vol. 12, no.15s, p.172-178, 2024.

[20] Yan, M., Cheng, Z., Gao, C., Sun, J., Liu, F., Sun, F. and Li, H., 2023. Cascading residual graph convolutional network for multi-behavior recommendation. *ACM Transactions on Information Systems*, *42*(1), pp.1-26.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[21] Balaji Singaram, M.S.Vinmathi, Dr.H.B.Michael Rajan, Jeyamohan H, T. Manikandan, "Data-Driven Estimation of Lithium-Ion Battery State-of-Health Prediction Approach Using Machine Learning Algorithm for Enhanced Battery Management Systems", Nanotechnology Perceptions, ISSN 1660-6795 2024, Vol: 20, 7s, 93-103.

[22] Guo, X., Wang, Y., Liu, H., Xie, H., Cheng, G. and Wang, F.L., 2023. Steerable Graph Neural Network on Point Clouds via Second-Order Random Walks. *IEEE Transactions on Multimedia*.

[23] Abdel-Basset, M., Mohamed, R., Azeem, S.A.A., Jameel, M. and Abouhawwash, M., 2023. Kepler optimization algorithm: A new metaheuristic algorithm inspired by Kepler's laws of planetary motion. Knowledge-based systems, 268, p.110454.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.