Egyptian Informatics Journal 22 (2021) 401–410

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system

Ramaprabha Jayaram *, S. Prabakaran

Department of Computer Science and Engineering, SRM Institute of Science & Technology, Kattankulathur, India

ARTICLE INFO

Article history:
Received 25 May 2020
Revised 28 October 2020
Accepted 11 December 2020
Available online 25 December 2020

Keywords:
Edge level security
Ambient assisted living
Adaptive probabilistic classifier
Cloud-based healthcare
Rehabilitation monitoring

ABSTRACT

Edge-based privacy preserving cryptosystem is identified as the upcoming amenities of cloud-based secure remote healthcare monitoring systems. Usually, the cloud-based healthcare system will directly collect the remote patient data through a sensor layer and provide the continuous monitoring and diagnosis through various prediction processes made by the decision support system. These sensing and processing of real-time patient's medical data without compromising its privacy and security become daunting issues in the traditional healthcare services. Therefore, the proposed research incorporates the security mechanism in the patient-centric edge-cloud-based healthcare system architecture. More precisely, an edge level privacy preserving additive homomorphic encryption is proposed for secure data processing and filtering non-sensitive data in the edge layer. In addition, response time and network capacity usage are minimized in the proposed healthcare system due to effective filtering and offloading mechanisms adapted in the edge level. Next, an adaptive weighted probabilistic classifier model is proposed in the cloud layer for onboard disease prediction and rehabilitation of remote patients. It will improve the disease prediction time and prediction accuracy while comparing to traditional classifier models. Finally, security and performance analysis of the proposed Secure Edge-Cloud-based Healthcare System (SECHS) was demonstrated with respect to empirical evaluation of Parkinson disease dataset.

1. Introduction

Cloud-based healthcare service became more popular due to centralized Electronic Healthcare Record (EHR) and uninterrupted service facility to patients remotely. Emerging tele-healthcare industry needs to maintain the security and privacy due to the growing nature of Healthcare 4.0 which has a significant impact on access mechanisms of patient data from common storage repositories [1]. In order to improve the coordination and enhancement of healthcare quality, patients can share their personal health records with doctors. The records are stored in cloud-based Zebra Health or Microsoft Health Vault [2]. Then, the doctor can make investigations on patients' health conditions based on the sequence of records stored in the cloud which gives the actual deviation in medical parameters. Due to this fact, the data stored in the cloud server will not have access to all medical data uploaded by multiple users which may be accidentally disclosed [3]. This situation will open the door of prying eyes to launch various levels of security attacks such as data privacy, integrity and confidentiality in healthcare systems. To provide security, an attribute based encryption scheme has been exploited to make access control on electronic healthcare records where the patient can decrypt the data using appropriate access policy [4]. Now-a-days, the edge-based healthcare services were employed for cost effective data processing and network resource provisioning on edge computing framework through data offloading and real-time processing respectively. Here, computational offloading at edge level can minimize the energy consumption, communication and computational delay between edge and cloud server [5]. Existing healthcare system research was focused more on data processing and data sharing security mechanisms at cloud server level [6,7]. Especially, integration of edge and cloud server platforms is very difficult for the real-time healthcare system to provide effective data processing and disease prediction. This is more evident from the edge-cloud integrated smart environment to improve people living quality over the cyber-physical system. Due to openness of the edge-cloud environment and limited access control of users,

* Corresponding author.
E-mail address: ramaprabhajayaram@gmail.com (R. Jayaram).

Peer review under responsibility of Faculty of Computers and Artificial Intelligence, Cairo University.

https://doi.org/10.1016/j.eij.2020.12.003
1110-8665/

there might be some inevitable cause leads to security issues like users privacy and providers business value [8]. In order to share the data to the end-user, more prevailing access control schemes are needed to improve the undesirable situation in the edge computing platform. More specifically some security threats like side channel attacks, virtualization vulnerabilities, networks eavesdropping and denial of service attacks are tightly associated with cloud data service [9]. Therefore, the healthcare data need to be encrypted locally before offloading and sharing among the peer-to-peer edge and cloud nodes. Moreover, the distortions of the signal due to the communication line and end-devices could be easily distinguished from the distortion of voice due to Parkinson disease. It can be identified by the low-volume voice having monotone quality of speech with unfortunate silences between words and extensive pauses prior to initiating speech.

To fill this research gap, an effective privacy preserving encryption scheme is introduced at edge and cloud server level. First objective of this research is to develop effective privacy preserving additive homomorphic encryption techniques and also energy aware live data offloading scheme at edge computing level. Next objective is to design and develop the adaptive weighted probabilistic classifier model in the cloud level for onboard disease prediction and rehabilitation monitoring purposes. Existing smart healthcare systems pertain to this research context was analyzed in both edge and cloud server level. In the edge level, an efficient and accountable access control framework was developed to make more secure and robust useful features for designing routers with slight delay on patient data retrieval [10]. A chaotic maps-based authentication scheme is employed in the edge computing level to realize the two factor data security and forward secrecy [11]. A decentralized property is enforced at cloud server level using blockchain technology, to ensure integrity and accountability of medical data stored in cloud environments [12]. In addition, blockchain technology helps to protect the information exchange between the cloud server and hospital network without any delay and information leakage. It promises to provide secure data storage and sharing among the medical stakeholders and remote patients with flexible data interoperability and payment modes [13]. It attains privacy of the data due to maintenance of cryptographic hash function of previous block, timestamp and transaction data. But it is limited to data index extraction overhead and cost effectiveness data processing transaction overhead on real-time smart contracts exploited in the healthcare system [14].

Apart from security, proposed research includes the implementation of adaptive classifier models in the edge-cloud-based healthcare system. Existing healthcare system exploited the reasoning-based privacy-aware decision support system for disease prediction and preservation of patient sensitive data [15]. A multistage classifier approach is implemented along with machine learning and particle swarm optimization based feature selection technique to improve the prediction accuracy and diagnosis of disease [16]. These approaches are more complex and increase the response time of the system, and obtain a very smaller fault alarm rate. To overcome these issues, the proposed research incorporates the privacy preserving additive homomorphic encryption and offloading mechanism to enhance the security and optimize the communication capacity and energy at edge level. Along with this encryption, the proposed research incorporates the adaptive weighted probabilistic classifier model at cloud server level for enhancing onboard disease prediction and rehabilitation monitoring process. The research paper is organized into five sections. Next section will provide a deep literature review of smart health care systems available in the cloud market according to the context of data security and disease prediction. Section 3, provides a detailed description of proposed edge-cloud-based healthcare system architecture with appropriate security and classifier model. In section 4, real-time experimental evaluation is briefly described along with evidence of resulting table and discussion. The closing section provides the research conclusion and future enhancement of the smart healthcare system.

2. Related works

2.1. Security in cloud based smart healthcare system

According to recent research studies in healthcare systems, various security mechanisms were adopted in both edge and cloud level as given in Fig. 1. At edge level, security techniques are applied in the context of cryptography, machine learning and computational intelligence approach [17]. Here, the cryptography approach includes the advanced encryption standard, secure sockets layer, access control, blockchain, cipher-text policy attribute-based encryption, decoy, Deffie-Hellman and Shibboleth security schemes. Next, the machine learning approach consists of deep learning, j48 decision and real-time machine security schemes. Finally, the computational intelligence approach contains various security schemes such as evolutionary game, fog-fisver and f-iov. Also a lightweight selective encryption scheme was developed based on a machine learning approach to further protect the patient data privacy [18]. A Canetti-Krawczyk security model is enforced in edge/fog level to establish secure communication between edge and cloud computing without leakage of any patient data identity [19]. Therefore, to bring rapid advancement in cyber-physical systems, a novel logarithmic encryption scheme was designed and verified for handling security, privacy and trust related issues in real environments [20]. To establish secure routing from source to destination, a trust detection-based secured routing scheme is established under a malicious environment for the sake of improving the success probability of routing in cyber-physical systems [21].

In cloud level, searchable public-key encryption scheme was used to balance the security and efficiency of search operations and also provides privacy protection over the encrypted data [22]. This scheme is extended as a fuzzy keywords enabled ranked searchable encryption scheme to guarantee the security features over a real-life speech corpus deployed on public cloud architecture [23]. Further, this searchable encryption cannot be a successful scheme until the search result falls into a precise time period. Therefore, a novel time-aware searchable encryption scheme is designed with designated medical cloud servers to provide more security and efficiency than the existing schemes [24]. A homomorphic encryption scheme was introduced to manage large-scale sensor data with high level privacy preserving anomaly detection service in cloud-based electronic health records [25]. A systematic review on various homomorphic encryption techniques such as fully, multiplicative, XOR, additive, and critical infrastructure homomorphic schemes were done to extend the healthcare application over big data and cloud environments. These techniques are used to manage and analyze the massive amount of heterogeneous medical data to further improve the quality of healthcare service [26]. According to literature study, some prominent schemes such as key policy attribute-based encryption, trust, multi-tenant, multi-authority, fine-grain, revocation mechanism, trace mechanism, proxy re-encryption and hierarchical encryption were analyzed for ensuring security and privacy in cloud [27].

Next, a quantum walks-based encryption was composed of substitution and permutation phases in healthcare systems for protecting the patients' privacy without compromising the robustness and efficiency of image encryption [28]. An authorized cloud server was protected with novel certificate less public-key

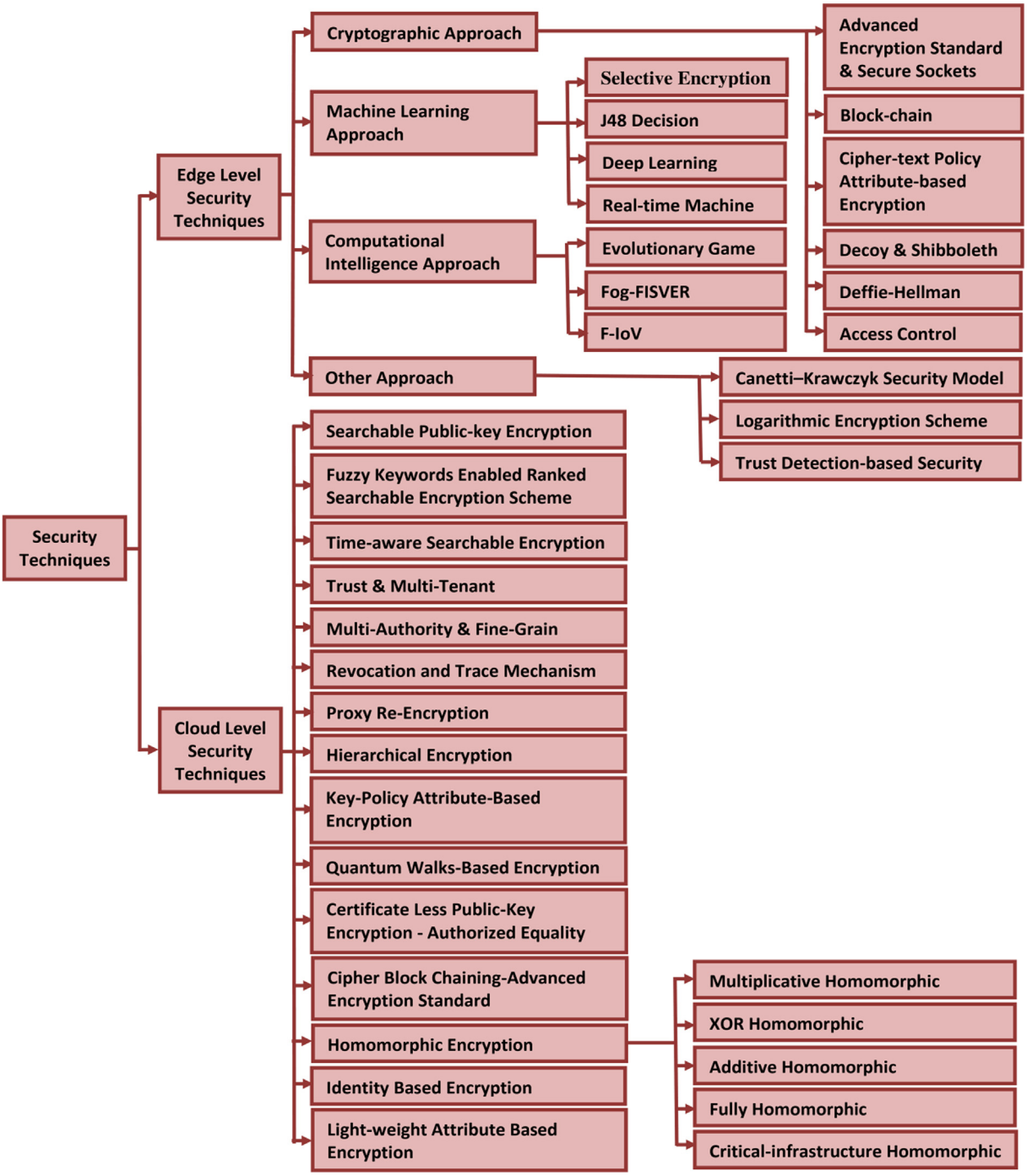

Fig. 1. Taxonomy of security techniques.

encryption along with authorized equality test scheme before outsourcing to smart healthcare service [29]. In order to improve the storage efficiency and data transfer safety between stakeholders, a cipher block chaining-advanced encryption standard is exploited along with Huffman coding and discrete wavelet transform [30]. A light-weight attribute based encryption was proposed to impose low overhead on proxy service based architecture with fine grained user revocation and access control capability over the mobile cloud assisted cyber-physical systems [31]. Finally, an identity based encryption scheme has been identified as a practical solution for one way security against the selected identity and cipher text attacks in random oracle model [32]. As per recent survey, all the above discussed security techniques are used to overcome various levels of threats such as audio steganography, botnet, denial of service, phishing, flooding request, malware injection and target shared memory attacks involved in both edge and cloud environment [33]. Therefore, the proposed research focuses on privacy preserving additive homomorphic encryption development to ensure secure data transfer and offloading computation at edge level.

2.2. Disease prediction classifier models

In the context of smart healthcare systems, different types of classifier models are used for real-time disease prediction and rehabilitation monitoring over edge and cloud computing platforms. In order to make early diagnosis of Parkinson disease, a comparative analysis was made using Naive Bayes, kernel-based support vector machine, random forest and boosted tree classifier models [34]. As a result, kernel-based support vector machine classifiers were observed as best performers in terms of prediction accuracy, sensitivity and specificity metrics. The modified k-NN classifier model has been applied in cancer disease prediction and diagnosis in the context of smallest and largest modification scenarios [35]. A fuzzy based k-NN classifier model was proposed to design an efficient diagnosis system for improving the performance of Parkinson disease detection [36]. Sometimes, the sensitivity of the k value may degrade the performance of the classifier in case of less sample size with traditional outliers. Therefore, a generalized mean distance-based k-NN classifier model was employed by estimating categorical nested and multi-generalized mean distances [37]. The accuracy of the classifier model will vary with respect to the types of feature extraction and optimization techniques. Since the voice and video data used for classifier training has its own pros and cons, the prediction accuracy of the model does not have much significant difference due to voice or video data exploitation. Therefore, the proposed research work shows the focus on developing adaptive weighted probabilistic classifier models for robust disease prediction and rehabilitation of remote patients with economical cost.

2.3. Comparison of healthcare system architectures

In the layered architecture context, very few research studies are present in the healthcare system with respect to two, three and four layer representation. The complete layered architectural comparison and analysis of healthcare systems are made in terms of security, interoperability and performance attributes as shown in Table 1. A cloud-based framework is designed with two layer healthcare architecture for Parkinson disease monitoring and diagnosis from remote place [38]. Next, a hierarchical fog-assisted computing architecture is designed with three layers for enhancing IoT based healthcare application [39]. Similarly, a fog based smart healthcare monitoring is presented with three layers for monitoring the human body vital signals like heart rate, respiratory rate, stress, temperature and pressure level [40]. But, this architecture does not make any prediction of disease and diagnosis over the patient data. An edge computing based smart healthcare system was introduced to optimize the healthcare operations and service flows with a simple data accessibility scheme. [41]. In order to provide interoperability among the healthcare systems, a semantic based healthcare interoperability framework is explored to provide secure information exchange [42]. While comparing the architecture of all the healthcare systems, the proposed secure edge-cloud-based healthcare system provides better security, interoperability and performance measurement attributes.

3. Proposed secure edge-cloud-based healthcare system

A layered architecture of secure edge-cloud-based healthcare system is proposed with edge level secure data filtering and offloading mechanism as presented in Fig. 2. The architecture entails voice/video sensor, edge computing and cloud computing layers. Voice/video sensor layer will lively capture the patient medical data from different movable locations of home. By smart phone it will sense the voice parameter and share the data to the edge layer. In case of video data, it will sense the patient data by using video surveillance cameras located at different locations through patient identification and tracking mechanisms. Then, the captured live medical data from the sensor layer will get initial processing at the edge computing layer where the privacy preserving additive homomorphic encryption is proposed to protect the sensitive data against the attackers. In edge level, the proposed architecture incorporates a microcontroller device called Raspberry Pi complete kit to enforce security and data offloading mechanism. This edge level device can optimize the response time and communication capacity usage between edge and cloud computing layers. The expected optimization is possible because non-sensitive data filtering happens during the offloading process which allows only needful medical data to be transferred to the cloud layer. In addition, the edge computing layer provides the computing and storage capability to collectively integrate all the medical data required for real-time disease prediction, diagnosis and rehabilitation monitoring over edge-cloud-based healthcare systems.

Next, the cloud computing layer providers secure and reliable processing and central storage platform for the healthcare system. Moreover, the data privacy and integrity is assured for all the healthcare services running on cloud-based virtual machine platforms. It provides the elasticity feature to the healthcare system by dynamically scaling up and scaling down virtual resources based on the number of on-demand user access available in the healthcare system. So, the cloud layer is employed to process all the offloaded data by referring to the patient's medical database available in cloud repository. Then the proposed adaptive weighted probabilistic classifier model will make the appropriate disease prediction based on the analysis of patient's past data and cur-

Table 1
Comparison of healthcare system architecture.

Healthcare Architectures	Layers	Security Schemes	Interoperability	Performance Attribute
Cloud-based framework	Consumer, Cloud	Base Level Data Security	No Interoperability	Prediction Time, Prediction Accuracy
Hierarchical fog-assisted computing architecture	Sensor, Fog, Cloud	No Security	No Interoperability	Response Time, Capacity Utilization, Quick Data Access
Fog-based smart healthcare monitoring	IoT, Fog, Cloud	No Security	No Interoperability	Quick Data Access
Edge computing based smart healthcare framework	User, Fog/Edge, Cloud	Data Accessibility	No Interoperability	Length of Stay, Resource Utilization, Patient Waiting Time
Semantic based healthcare interoperability framework	Smart-Device, Fog, Cloud	Base Level Data Security	Interoperability	Restful Protocol
Fog computing based preventive healthcare	Interaction, Mesh, Fog, Cloud	Trust based Security	No Interoperability	Interoperability
Proposed secure edge-cloud-based healthcare system	Sensor, Edge, Cloud	Additive Homomorphic Encryption	Interoperability	Prediction Time, Prediction Accuracy, Response Time, Capacity Usage

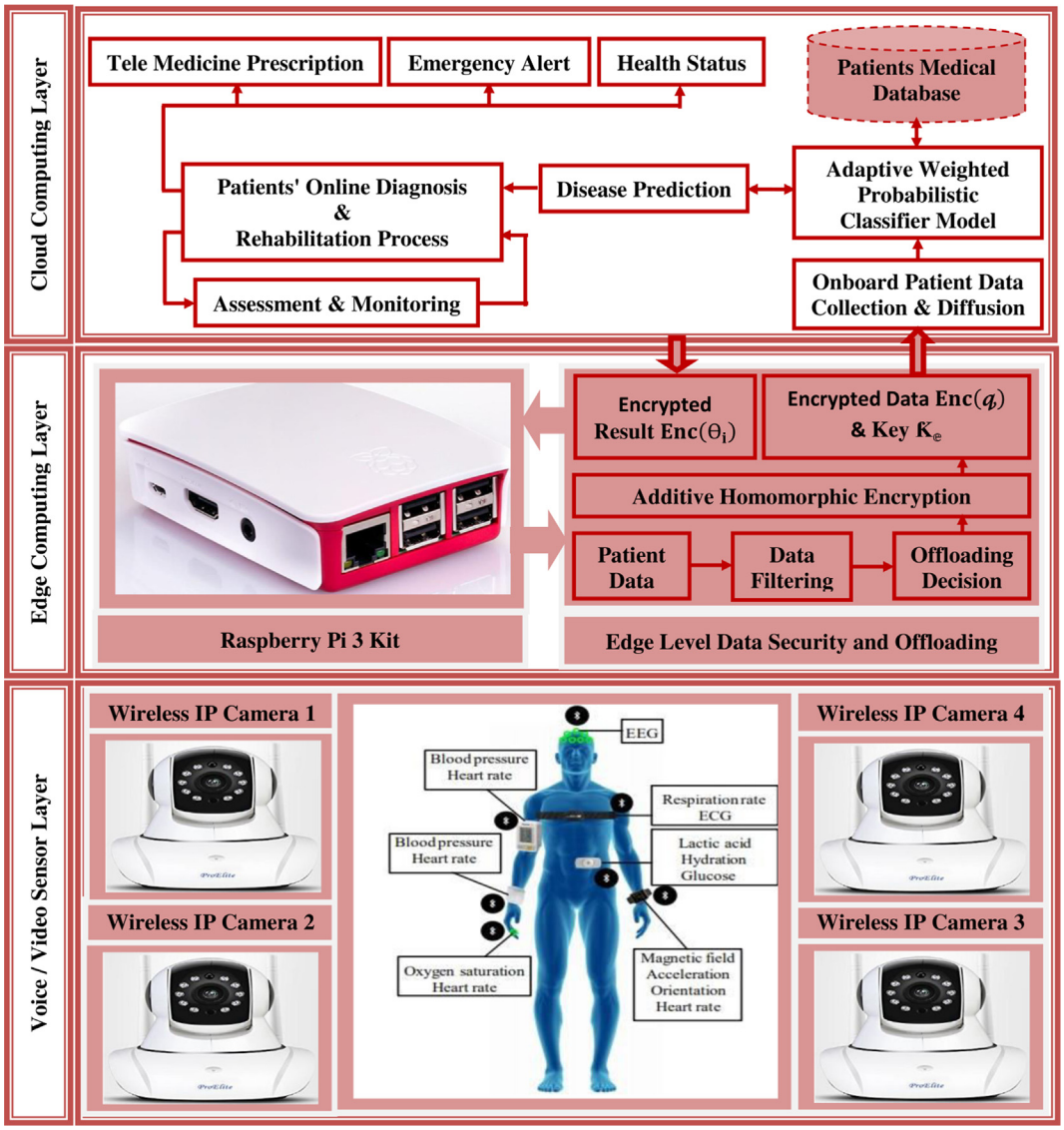

Fig. 2. Secure Edge-Cloud-based Healthcare System Architecture.

rently sensed data. Finally, the healthcare system can start the online diagnosis and rehabilitation process based on the severity level of patients. A continuous monitoring and assessment of Parkinson disease related parameters will identify the deviations happening in the patient's health condition during rehabilitation processes. Based on the improvements observed during the rehabilitation process, the health status and Tele medicine prescription will be automatically disclosed to the patient and caretaker. In case of abnormal health conditions, an emergency alert will be given to the corresponding doctor and caretaker. Also, additional medical and care giving services can be given based on the online subscription and predefined health policy activated by the remote patient.

3.1. Problem formulation of edge level filtering and offloading decisions

After sensing medical data from the sensor layer, an edge level data filtering and offloading process is done through appropriate mechanisms. To construct edge level security, a privacy preserving cryptosystem comprised data encryption and data decryption over the encrypted tensor proposed in the integrated secure edge-cloud-based healthcare system architecture. Initially, the data filtering scheme is adopted to filter all the non-sensitive data in the edge node and offload only the sensitive data to cloud computing nodes available in the C_{Layer}. Therefore, the offloading problem can be defined with n number of edge computing nodes $EN = \{EN_1, EN_2, \cdots, EN_n\}$ as shown in equation (1). Then, the minimization of offloading function $\mathcal{Z}(EN)$ is described in equation (2) with constraints such as $\sum_{i=1}^{n} EN_i = DO$, $EN_i \leq \mathcal{SLA}_i$ and $EN_i \geq 0$. Let $\mathcal{SLA}_i$ be the service level agreement parameter be enforced on edge nodes and DO be the total amount of patient data tasks need to be offloaded to cloud computing nodes available in C_{Layer} i.e., $DO = V^{P}_{Total}$.

$$Min_{EN}\, \mathcal{Z}(EN) \tag{1}$$

$$\mathcal{Z}(EN) = \sum_{i=1}^{n} \omega * \mathcal{T}_{off}(EN_i) + (1-\omega) * \varepsilon_{off}(EN_i) \tag{2}$$

where ω be the weighting parameter of offloading transmission time and energy consumption, $\mathcal{T}_{off}$ be the offload transmission time and ε_{off} be the offload energy consumption of edge node EN_i during offloading activity. Here, the offload transmission time at any time

stamp τ can be measured based on the size of computable input data V_i and uplink data rate $\mathcal{R}_{UpLink}$ as given in equation (3).

$$\mathcal{T}_{off}(EN_i) = \frac{V_i{}^{\tau}}{\mathcal{R}_{UpLink}{}^{\tau}} \tag{3}$$

Similarly, the offload energy consumption at edge node EN_i can be measured as formulated in equation (4). Let ε_{Tail} denote the tail energy to hold the communication channel even after data transmission and $\mathcal{P}_{\mathcal{T}}$ denote the offload transmission power of edge nodes EN_i.

$$\varepsilon_{off}(EN_i) = \frac{\mathcal{P}_{\mathcal{T}} V_i{}^{\tau}}{\mathcal{R}_{UpLink}{}^{\tau}} + \varepsilon_{Tail} \tag{4}$$

In order to satisfy the committed $\mathcal{SLA}_i$ at C_{Layer}, the total energy consumption and network delay of correspond cloud node should be minimized for improve the response time of proposed healthcare system. This improvement can be made possible by minimizing the delay and network capacity incurred by edge level offloading process. Accordingly, estimate the allocation of network capacity between EN_i and cloud nodes CN_j by using equation (5).

$$\beta_{EN_i \leftrightarrow CN_j} = \frac{\beta_{EN_i}(\pi_{EN_i})}{\pi_{EN_i}} \tag{5}$$

where π_{EN_i} be the offloading capacity of edge nodes $EN_{i\in(1,n)}$, and $\beta_{EN_i}(\pi_{EN_i})$ represents the amount of network capacity among the edge nodes shared by the corresponding cloud node CN_j. The total delay $\mathcal{D}$ to serve the patient data offloading request at time period τ can be formulated as shown in equation (6). Here, the binary variable $\varphi^{\tau}_{V_i}$ should be used to characterize whether the cloud node CN_j can serve the data request of the edge node EN_i or not.

$$\mathcal{D}^{\tau}_{Total} = \mathcal{D}^{\tau}_{EN_i \leftrightarrow CN_j} + \mathcal{Q}^{\tau}_{EN_i \leftrightarrow CN_j} \varphi^{\tau}_{CN_j} + \mathcal{Q}^{\tau}_{EN_i \leftrightarrow CN_j}(1 - \varphi^{\tau}_{CN_j}) \tag{6}$$

However, the delay incurred to transfer patient medical data from edge node EN_i to cloud node CN_j can be computed as given in equation (7).

$$\mathcal{D}^{\tau}_{EN_i \leftrightarrow CN_j} = \frac{\delta^{\tau}_{V_i}}{\beta_{EN_i \leftrightarrow CN_j}} + \frac{\mathscr{A}^{\tau}_{EN_i \leftrightarrow CN_j}}{\mathscr{P}^{\tau}_{EN_i \leftrightarrow CN_j}} \tag{7}$$

Let $\delta^{\tau}_{V_i}$ be the size of patient medical data request to be processed in time slot τ, $\mathscr{A}^{\tau}_{EN_i \leftrightarrow CN_j}$ be the strength of signal decay between edge node EN_i and cloud node CN_j, and $\mathscr{P}^{\tau}_{EN_i \leftrightarrow CN_j}$ be the propagation speed of communication medium established between EN_i and CN_j. Next, the queuing delay in the cloud node CN_j to process the patient data request received from edge nodes EN_i can be estimated using equation (8).

$$\mathcal{Q}^{\tau}_{EN_i \leftrightarrow CN_j} = \mathcal{T}^{\tau}_{CN_j} - \frac{1}{\mu^{\tau}_{CN_j}} \tag{8}$$

where $\mathcal{T}^{\tau}_{CN_j}$ denotes the average amount of time spent by patient data in cloud node CN_j, and $\mu^{\tau}_{CN_j}$ denotes the number of patient data request served in cloud node CN_j at time slot τ.

3.2. Edge-cloud-based secure healthcare system modeling by additive homomorphic encryption

After data filtering at edge nodes, offloading decisions will initiate the privacy preserving cryptosystem to ensure the privacy and security during the offloading of patient data from edge node to cloud node. Therefore, the sequence of past and present medical data sensed from patient's are periodically encrypted and offloaded to cloud node available at C_{Layer}. Assume the patients query vector $\mathscr{q} = \{\mathscr{q}_1, \mathscr{q}_2, \cdots, \mathscr{q}_n\}$ denotes the set of patients query with their respective medical data $V = \{V_1, V_2, \cdots, V_n\}$. This query vector includes the necessary features of disease diagnosis and also needs to be clearly determined by the trait vector of the healthcare system. Then the cloud layer will present the medical database $\hat{D} = \{\hat{D}_1, \hat{D}_2, \cdots, \hat{D}_n\}$ of patients as quadruple as given in equation (9), based on the sequence of previously sensed medical data.

$$\hat{D}_i = \mathrm{I}_i, C_i, T_i, \Theta_i \tag{9}$$

where I_i represent the index of disease D_i, C_i indicates the cipher text, T_i be the trait vector of disease D_i that includes the multi-dimensional data vector of all the features required for the diagnosis and rehabilitation of disease, Θ_i denotes the final diagnostic output of healthcare system which includes disease name, clinical manifestation and doctor prescriptions related to disease D_i.

The healthcare system in C_{Layer} will maintain the trait vectors $\mathrm{T}_i = (\mathrm{t}_{i1}, \mathrm{t}_{i2}, \cdots, \mathrm{t}_{in})$ of disease repository for identifying the deviation of medical features after diagnosis and rehabilitation process by continuously matching the current state of patient data trait vectors with past states of trait vectors available in disease repository. In order to identify the deviation of medical features between the trait vectors of patient query q and disease repository D_i, an Euclidean distance is measured as shown in equation (10).

$$d(q, \mathrm{D}_i) = \| q - \mathrm{D}_i \|^2 \tag{10}$$

Due to the expansion of distance parameter evaluation such as $q - \mathrm{D}_i^2 = (q_1 - t_{i1})^2 + (q_2 - \mathrm{t}_{i2})^2 + \ldots + (q_n - \mathrm{t}_{in})^2$, the equation (10) can be rewritten as equation (11).

$$d(q, \mathrm{D}_i) = \sum_{j=1}^{n} q_j^2 + \sum_{j=1}^{n} \mathrm{t}_{ij}^2 + \sum_{j=1}^{n} (-2 q_j \mathrm{t}_{ij}) \tag{11}$$

Then, the complete similarity between the trait vectors of patient query $\mathscr{q}$ and disease repository D_i is formulated as shown in equation (12).

$$Sim(q, \mathrm{D}_i) = \frac{1}{1 + d(q, \mathrm{D}_i)} \tag{12}$$

Here, the similarity range [0,1] denotes the distance closer where higher similarity value indicated less deviations in trait vectors of patient (less improvements on diagnosis) and smaller similarity value indicated more significant deviations in trait vectors of patient (more improvements on diagnosis). According to deviation in similarity value, the doctor will change the diagnosis and rehabilitation process until there are some improvements observed from the trait vectors of patient data during subsequent monitoring states.

In order to maintain the patient's privacy, an additive homomorphic encryption scheme is employed to encrypt the trait vectors of patient data and disease repository data from edge and cloud layer as $Enc(q)$ and $Enc(\mathrm{T}_i)$ respectively. Therefore, first generates the key pairs $(\mathrm{K_e}, \mathrm{K_d})$ for initiating the additive homomorphic encryption over the trait vectors of patient data. Then, the healthcare system uses the encryption key $\mathrm{K_e}$ to encrypt the patient data query q as $Enc(q) = (Enc(q_1), Enc(q_2), \cdots, Enc(q_n))$. Finally, the edge node will send the cipher text of patient data $\mathrm{C}_i = Enc(q)$ along with the encryption key $\mathrm{K_e}$ to the cloud layer. Afterwards, the healthcare system will perform the homomorphic encryption computation given in equation (13) and (14) based on the trait vectors of disease repository T_i and the cipher text $Enc(q)$ received from the patient with corresponding encryption key $\mathrm{K_e}$.

$$M_2 = Enc\left(\sum\nolimits_{j=1}^{n} \mathrm{t}_{ij}{}^2\right) \tag{13}$$

$$M_3 = Enc\left(\sum\nolimits_{j=1}^{n} (-2\mathscr{q}_j \mathrm{t}_{ij})\right) = \Pi_{j=1}^{n} Enc(q_j)^{-2\mathrm{t}_{ij}} \tag{14}$$

To further prevent other stakeholders from obtaining the privacy information of cipher text $Enc(q)$, a set of random numbers are generated by the patient to form n-dimensional vector as $\mathcal{H} = \{\mathcal{H}_1, \mathcal{H}_2, \cdots, \mathcal{H}_n\}$. These random numbers of $\mathcal{H}$ will make some disturb in the information of $\mathcal{G}$. Then, the patient will be computed $\mathbb{s} = Enc\left(\sum_{j=1}^{n} \alpha_j{}^2\right)$ and sent to the healthcare system for getting further diagnosis and rehabilitation from the doctor where $\alpha_j = \mathcal{G}_j + \mathcal{H}_j$. At last, the healthcare system computes the $\mathcal{M}_1$ as shown in equation (15). Then, the encrypted distance measure $Enc(\mathrm{D}_i)$ is computed as given in equation (16) and sent to the patient.

$$M_1 = \mathbb{s} \cdot \Pi_{j=1}^{n}\left(Enc\left(\mathcal{G}_j\right)^{-2\mathcal{H}_j} \cdot Enc\left(-\mathcal{H}_j^2\right)\right) = Enc\left(\sum\nolimits_{j=1}^{n} \mathcal{G}_j{}^2\right) \tag{15}$$

$$Enc(\mathrm{D}_i) = M_1 \cdot M_2 \cdot M_3 \tag{16}$$

After substituting the value of $\mathcal{M}_1$, $\mathcal{M}_2$ and $\mathcal{M}_3$ in equation (16), the summative encryption is obtained as composed in equation (17).

$$Enc(\mathrm{D}_i) = Enc\left(\sum\nolimits_{j=1}^{n} \mathcal{G}_j{}^2 + \sum\nolimits_{j=1}^{n} \mathrm{t}_{ij}{}^2 + \sum\nolimits_{j=1}^{n} (-2\mathcal{G}_j \mathrm{t}_{ij})\right) \tag{17}$$

After estimating encrypted distance measure (D_i), the healthcare system will decrypt $Enc(\mathrm{D}_i)$ as D_i and compute the similarity function $Sim(\mathcal{G}, \mathrm{D}_i)$ to determine the deviations of trait vectors of patient and disease repository. Then predict the Parkinson disease severity using the adaptive weighted probabilistic classifier model and choose the best diagnostic method suggested by the healthcare system through proper encryption $Enc(\Theta_i)$ with the respective patients. Finally, the remote patient can decrypt the obtained result Θ_i to undergo further diagnosis and rehabilitation process given by the doctor.

3.3. Disease prediction and rehabilitation in healthcare system using adaptive weighted probabilistic classifier model

The healthcare service provisioning from cloud layer has effective storage and processing capability for real-time disease prediction and rehabilitation process by exploiting the proposed adaptive weighted probabilistic classifier model. After receiving the patient's data requests from various geographic regions, the proposed classifier will be exploited by the healthcare system for quick prediction and response generation to concern. At cloud layer C_{Layer}, there are n number of live data request $V_{i\in(1,n)}$ were received to process in the classifier service which in turn parallelize the data processing task to m number of virtual machines $VM_{j\in(1,m)}$. A classifier service hosted at each VM can have a maximum VM_{DP}^{Max} and minimum VM_{DP}^{Min} bound of data processing capability for processing the corresponding maximum V_i^{Max} and minimum V_i^{Min} amount of data tasks respectively. Now, the objective of research is to minimize the cost of VM provisioning initiated for data processing at classifier service hosted in C_{Layer} as defined in equation (18).

$$Minimize\ \mathcal{C}_{Total}(V_i) + E\left[p\left(V_{Total}^{P} - V_{Total}^{VM}\right)\right] \tag{18}$$

Let $\mathcal{C}_{Total}$ represents the total cost of processing data task $V_{i\in(1,n)}$, V_{Total}^{P} denotes the total data service demanded by the remote patients and V_{Total}^{VM} denotes the overall data service obtainable from all possible $VM_{j\in(1,m)}$ at time τ. Finally, $E\left[p\left(V_{Total}^{P} - V_{Total}^{VM}\right)\right]$ represents the expected cost of buying healthcare service from C_{Layer} to accomplish the total data service demanded of remote patients. A sample average approximation method is applied to solve this portfolio optimization problem due to its stochastic nature and expected value constraints. It can be formulated using the set of samples $S_{k\in(1,n)}$ applied through joint distribution of total data service request and VM availability as given in equation (19).

$$\mathcal{C}_{Total}(V_i) + \frac{1}{n}\sum_{k=1}^{n} p * \left(V_{Total}^{P}(S_k) - V_{Total}^{VM}(S_k)\right) \tag{19}$$

Thus, the above sample average approximation solution of optimization problem can redefine the objective function of (18) as shown in equation (20). The corresponding constraints are defined as $V_i \geq V_i^{Min}$, $V_i \leq V_i^{Max}$ and $V_{Total}^{VM} \leq V_{Total}^{P}$. Due to sample selection this solution may arrive at a near optimal result. Therefore, the validation set $(\widehat{V}_{Total}^{P}, \widehat{V}_{Total}^{VM})$ is exercised to test the optimal solution validity with respect to the total validation sample $S_{k\in(1,n)}^{Val}$. As a result, the validity checking optimization solution of sample average approximation can be defined as given in equation (21) with respect to constraint $\widehat{V}_{Total}^{VM} \leq \widehat{V}_{Total}^{P}$.

$$Minimize\left[\mathcal{C}_{Total}(V_i) + \frac{1}{n}\sum_{k=1}^{n} p * \left(V_{Total}^{P}(S_k) - V_{Total}^{VM}(S_k)\right)\right] \tag{20}$$

$$Minimize\left[\mathcal{C}_{Total}(V_i) + \frac{1}{n}\sum_{k=1}^{n} p * \left(\widehat{V}_{Total}^{P}\left(S_k^{Val}\right) - \widehat{V}_{Total}^{VM}\left(S_k^{Val}\right)\right)\right] \tag{21}$$

The equivalent certainty of sample average approximation solution can be formulated as given in equation (22). Similarly, the validity checking of equivalent certainty solutions can be derived with the same constraints as given in equation (23) using the optimization approach.

$$Minimize\left[\mathcal{C}_{Total}(V_i) + p * Max\left(0, \left(Average\left(V_{Total}^{P}\right) - Average(V_{Total}^{VM})\right)\right)\right] \tag{22}$$

$$Minimize\left[\mathcal{C}_{Total}(V_i) + p * Max\left(0, \left(Average\left(\widehat{V}_{Total}^{P}\right) - Average(\widehat{V}_{Total}^{VM})\right)\right)\right] \tag{23}$$

At any time stamp $\Delta\tau$, the proposed healthcare system can predict the disease severity of patient data V_i during the state of rehabilitation assessment and monitoring activity as formulated in equation (24).

$$P_{Disease}^{\Delta\tau}(V_i) = Max\Pi_{k=1}^{L} P\left(\mathcal{F}_k^{\tau} | SI_{\mathcal{F}}\right) \tag{24}$$

Let L denotes the length of time spent by the patient data on cloud layer during prediction, $\mathcal{F}_k^{\tau}$ denotes the observed characteristic feature of disease at time τ, and $SI_{\mathcal{F}}$ be the severity indicator of feature assessed during rehabilitation process. The positive and negative probability value of experiencing the disease severity under the observed feature $\mathcal{F}$ are given as $P(\mathcal{F}|\mathcal{S}_+)$ and $P(\mathcal{F}|\mathcal{S}_-)$ with respect to threshold value Φ. Next, the weighted prior probability of feature $\mathcal{F}$ at time stamp $\Delta\tau$ can be measured as defined in equation (25).

$$P_W^{\Delta\tau}(\mathcal{F}|\mathcal{S}_+) = P\left(\mathcal{F}^T\right) * P\left(\mathcal{F}^T|\mathcal{S}_+\right) \tag{25}$$

Similarly, the weighted posterior probability function can infer the value as defined in equation (26) and (27). Let $W(\mathcal{F}^{\tau})$ represents the weight of various voice features such as jitter, shimmer, harmonics-to-noise ratio, noise-to-harmonics ratio, normalized noise energy and so on.

$$P_W^{\Delta\tau}(\mathcal{S}_+|\mathcal{F}) = P_W(\mathcal{F}^{\tau}|\mathcal{S}_+) * P(\mathcal{S}_+)P(\mathcal{F}^{\tau}) \tag{26}$$

$$P_W^{\Delta\tau}(\mathcal{S}_+|\mathcal{F}) = W(\mathcal{F}^{\tau}) * P(\mathcal{F}^{\tau}|\mathcal{S}_+) * P(\mathcal{S}_+)P(\mathcal{F}^{\tau}) \tag{27}$$

Here, the value of $P(\mathcal{F}^{\tau})$ can be expressed as given in equation (28) and (29).

$$P(\mathcal{F}^{\tau}) = P_W(\mathcal{F}^{\tau}|\mathcal{S}_+)P(\mathcal{S}_+) + P(\mathcal{F}^{\tau}|\mathcal{S}_-)P(\mathcal{S}_-) \tag{28}$$

$$P(\mathcal{F}^{\tau}) = W(\mathcal{F}^{\tau})P(\mathcal{F}^{\tau}|\mathcal{S}_+)P(\mathcal{S}_+) + P(\mathcal{F}^{\tau}|\mathcal{S}_-)P(\mathcal{S}_-) \tag{29}$$

Finally, the severity indicator value $SI_{\mathcal{F}}^{\Delta\tau}$ is estimated as formulated in equation (30) based on the number of features observed from the patient data during time stamp $\Delta\tau$. Therefore, the aggregated heterogeneous activity of patient data V_i is formulated for disease severity identification as given in equation (31).

$$SI_{\mathcal{F}}^{\Delta\tau} = \frac{1}{k}\sum_{\mathcal{F}} P_W^{\Delta\tau}(\mathcal{S}_+|\mathcal{F}) \tag{30}$$

$$P_{Disease}^{\Delta\tau}(V_i) = Argmax_{k=1,2,\cdots,L} P\left(SI_{\mathcal{F}}^{\Delta\tau}\right)\Pi_{k=1}^{L} P\left(\mathcal{F}_k^{\tau}|SI_{\mathcal{F}}\right) \tag{31}$$

Prediction Accuracy $P_{Disease}^{Accuracy}$ can be defined by the ratio of properly classified incidence to the total presented incidence as given in equation (32).

$$P_{Disease}^{Accuracy} = \frac{T^+ + T^-}{T^+ + F^+ + T^- + F^-} \tag{32}$$

Where T^+, T^-, F^+ and F^- represents the quantity of true positives, true negatives, false positives and false negatives respectively. Also the prediction time is estimated based on time of submission of request and final prediction response obtained from the healthcare system. After disease severity prediction, the healthcare system will choose the best online diagnosis and rehabilitation monitoring service for each patient. Then, the patient can decrypt and follow the diagnosis and rehabilitation methods Θ_i suggested by the doctor. Also the system will periodically monitor and assess the disease diagnosis and rehabilitation process to identify the feature $\mathcal{F}^T$ improvements of patients over the observed time period. According to feature improvements, the healthcare system can change the diagnostic method based on the alteration of onboard health status, Telemedicine prescription, healthcare service privileges and emergency alert situations.

4. Experimental evaluation

4.1. Experimental settings

The real-time experimental settings of the proposed SECHS model is evaluated by including edge level filtering and offloading mechanism. A remote patient data is lively captured through the healthcare app from 4 camera devices located in different places of home. Each camera device and healthcare app are connected to a nearby edge computing node called Raspberry Pi complete kit device. First, the camera device specification includes ProElite IP01A IP with 4G enabled network and Wi-Fi capability to capture high definition video data. Next, the Raspberry Pi kit specification includes 1 GB RAM capacity, 1.2 GHz processing speed, BCM43143 Wi-Fi and Bluetooth Low Energy (BLE) on board capabilities. Here, the pi-3 kit will do filtering and offloading on lively captured voice data and then follow the additive homomorphic encryption for maintaining the patient data privacy. After encryption, the edge node will send the encrypted data and key to the cloud computing node. Again, the proposed SECHS will decrypt the patient data and process the data in the proposed adaptive weighted probabilistic classifier which is deployed in the cloud computing node. Finally, the classifier will make effective disease severity prediction and provides the patient with online rehabilitation monitoring and assessment capability. In order to evaluate the performance of the proposed SECHS and its adaptive weighted probabilistic classifier model, a comparative analysis is made with existing research in terms of network capacity utilization, response time, prediction time and prediction accuracy. Initially, the classifier is trained with two benchmarking voice dataset taken from University of California-Irvine (UCI) repository [43,44]. The training dataset has sound recordings of 195 voice samples, out of which 147 samples affected and 48 samples not affected by Parkinson disease respectively. Those voice samples were collected from 31 subjects (8 healthy and 23 Parkinson affected patients). After training the classifiers with samples, an effective comparative analysis is made with respect to prediction time and prediction accuracy parameters to test the efficiency of both proposed and existing classifiers. Then, during the patient data prediction, an average performance of 5 experimental trails are tabulated for the results and discussion.

4.2. Results and discussion

The proposed SECHS performance is measured by comparing with existing healthcare systems such as Smart Architecture for in Home Healthcare (SAHH) and IoT-based Healthcare Smart Homes (IHSH) in terms of network capacity and response time. Results obtained during the experimentations are given in Table 2. More clear from the tabulated observation, the proposed SECHS model takes only less network capacity of 130 (kbps) while comparing to existing SAHH and IHSH systems which takes maximum network capacity of 350 (kbps). Since the proposed SECHS filters all the unwanted features of patient data, it minimizes the network capacity utilization in the edge level itself. Therefore, the proposed SECHS offloads only sensitive patient data to cloud nodes for initiating the disease severity prediction and rehabilitation assessment by continuous monitoring. As a result, the proposed SECHS takes very less response time (80 s) while compared to existing SAHH (120 s) and IHSH (170 s) systems.

An effective comparison is made between the proposed adaptive weighted probabilistic classifier with existing classifiers such as Neural Network, Linear Kernel SVM, Polynomial Kernel SVM, Radial Basis Kernel SVM and Sigmoidal Kernel SVM in terms of prediction time and accuracy. According to obtained results given in Table 3, the proposed adaptive weighted probabilistic classifier model outperforms the existing classifiers in both aspects. Therefore, the adaptive weighted probabilistic classifier obtains more robust performance due to the cloud-based deployment and efficiency of adaptive probabilistic approach employed during disease prediction and rehabilitation process.

In order to evaluate the security feature, the proposed additive homomorphic encryption scheme is compared against the existing privacy-preserving self helped medical diagnosis [45] and Boneh-Goh-Nissim homomorphic cryptosystem [46] schemes as given in Table 4. Since the proposed additive homomorphic encryption scheme is proved to be semantically secure, it could easily defend against the chosen plaintext attack and also it produces the semantically secure parameters. However, the other existing schemes can also defend against the chosen plaintext attack, but it could be easily cracked within some time period. So, the existing schemes cannot be complete resistant for the chosen plaintext attack. Next, there is no defending capability for the existing Boneh-Goh-Nissim homomorphic cryptosystem scheme, but the proposed additive homomorphic encryption scheme can provide more security in

Table 2
Performance measure of healthcare systems.

Healthcare Systems	Network Capacity (Kbps)	Response Time (Seconds)
IHSH	350	170
SAHH	350	120
Proposed SECHS	130	80

Table 3
Performance measure of classifier models.

Classifier Models	Prediction Time (Seconds)	Prediction Accuracy (Percentage %)
Neural Network	2.10409	92.5
Linear Kernel SVM	0.00370	89.7
Polynomial Kernel SVM	0.00174	79.5
Radial Basis Kernel SVM	0.00197	79.5
Sigmoidal Kernel SVM	0.00289	79.5
Proposed Adaptive Weighted Probabilistic	0.00107	96.9

Table 4
Performance measure of security schemes.

Types of Security Schemes	Types of Defending Against Attacks			
	Plain Text Attack	Collusion Attack	External Eavesdropping Attack	Replaying Attack
Privacy-preserving self helped medical diagnosis	No	Yes	Yes	No
Boneh-Goh-Nissim homomorphic cryptosystem	Yes	No	Yes	No
Proposed additive homomorphic encryption	Yes	Yes	Yes	Yes

both edge and cloud platforms without any collusion attack. In case of eavesdropping attack, all the schemes have defending capability due the assumption of secure transmission of data among the stakeholders. Even then, the proposed scheme has more security feature capability due to the exploitation of privacy preserving secure communication protocol in the healthcare system. Finally, the proposed additive homomorphic encryption scheme provides the identity authentication feature in the privacy preserving communication protocol. Therefore, the proposed scheme can defend against the replaying attack, where the existing scheme does not involve any patient's identity feature to defend against the replaying attack. Since the proposed additive homomorphic encryption scheme introduces an identity based authentication mechanism with added timestamp features can make significant improvement in the privacy preserving access control part. The healthcare system not only verifies the cipher-text during data transmission but also verifies the freshly generated timestamp in each transmission. In order to improve the diagnosis level, all the hospitals continue to have diverse trait vectors at different times. After receiving the patient data, originality of the timestamp associated with data is verified by comparing the timestamp present in the encrypted data to ensure protection against replaying attacks. Therefore, the proposed scheme involves the timestamp during the patient's identification and provides resistance against the replaying attack.

The computation processing cost of patient data on the proposed SECHS is measured by mapping with *d*dimensional vector representation of electronic health record available in database repository. Here, the encryption cost of patient data during the generation of cipher text $Enc(\wp)$ and random numbers $\mathcal{H}$ includes $\mathcal{O}(d^3)$ and $\mathcal{O}(d^2)$ costs respectively. Next, the transmission cost of n number of encrypted data to the cloud node is $\mathcal{O}(n * d^2)$. Prediction system setting complexity is measured as $\mathcal{O}(n * d^3)$ dependent on n number of trait vectors $\AA^{|}_{|_i}$ present in the medical database $\dot{D}$. Then, the time complexity of diagnosis and rehabilitation monitoring of patients on cloud nodes is $\mathcal{O}(m * d^3)$, where m represents the number of probabilistic prediction models employed during disease prediction. Final prediction result is represented in the index of disease D_i with cost as $\mathcal{O}(k)$. In future, the research work can be extended with NVIDIA deep learning server capability to dramatically improve the response time of predictions made in cloud datacenter. In case of implementing proposed solutions by adding a fog layer may provide better performance on patient disease prediction due to sharing of computational workloads among the real-time fog routers and cloud nodes [47]. As a result, an hierarchical disease prediction mechanism can be enforced through peer-to-peer communication and data offloading among the fog routers and cloud nodes.

5. Conclusion and future enhancement

In this research, a layered architecture of secure edge-cloud-based healthcare system is presented for real-time disease prediction with diagnosis and rehabilitation facility. The proposed system incorporates privacy preserving additive homomorphic encryption to ensure the data security at the edge computing layer. Also minimizes the response time and network capacity between the edge and cloud layers by using effective filtering and offloading mechanisms. All the patient data requests from different geographic locations were processed in a cloud layer using the proposed adaptive weighted probabilistic classifier model. The cost of resource provisioning at the cloud layer is minimized due to optimal resource usage of the proposed adaptive weighted probabilistic model during the processing of patient data tasks. To validate the performance of proposed secure edge-cloud-based healthcare systems, a comparative analysis is made with existing systems in terms of prediction time, prediction accuracy, response time and capacity usage. According to obtained results, it can be concluded more evidently that the proposed healthcare system significantly outperforms all the existing systems compared during experimental evaluation. However, some important challenges like edge-to-edge secure object tracking and transmission protocol must be dealt in future research. In addition, blockchain enabled security features can be applied in the cloud layer for effective privacy preservation of patients' electronic healthcare records.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput Commun 2020;153:311–35. doi: https://doi.org/10.1016/j.comcom.2020.02.018.
[2] Liang J, Qin Z, Xiao S, Zhang J, Yin H, Li K. Privacy-preserving range query over multi-source electronic health records in public clouds. J Parallel Distrib Comput 2020;135:127–39. doi: https://doi.org/10.1016/j.jpdc.2019.08.011.
[3] Liu J, Ma J, Wu W, Chen X, Huang X, Xu Li. Protecting mobile health records in cloud computing: a secure, efficient, and anonymous design. ACM Trans. Embed. Comput. Syst. 2017;16(2):1–20. doi: https://doi.org/10.1145/2983625.
[4] Liu Yi, Zhang Y, Ling J, Liu Z. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. Future Generation Computer Systems 2018;78(3):1020–6. doi: https://doi.org/10.1016/j.future.2016.12.027.
[5] Lin K, Pankaj S, Wang Di. Task offloading and resource allocation for edge-of-things computing on smart healthcare systems. Comput Electr Eng 2018;72:348–60. doi: https://doi.org/10.1016/j.compeleceng.2018.10.003.
[6] Zhang C, Zhu L, Chang Xu, Rongxing Lu. PPDP: an efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system. Future Generation Computer Systems 2018;79(1):16–25. doi: https://doi.org/10.1016/j.future.2017.09.002.
[7] Hadian M, Altuwaiyan T, Liang X, Li W. Privacy-preserving voice-based search over mHealth data. Smart Health 2019;12:24–34. doi: https://doi.org/10.1016/j.smhl.2018.04.001.

[8] Feng J, Yang LT, Zhang R. Practical privacy-preserving high-order bi-lanczos in integrated edge-fog-cloud architecture for cyber-physical-social systems. ACM Trans Internet Technol 2019;19(2):1–18. doi: https://doi.org/10.1145/3230641.
[9] Rabindra K. Barik, Harishchandra Dubey, Kunal Mankodiya, SOA-FOG: Secure service-oriented edge computing architecture for smart health big data analytics, IEEE Global Conference on Signal and Information Processing, Montreal, QC, Canada, 2017. doi: 10.1109/GlobalSIP.2017.8308688.
[10] Xue K, He P, Zhang X, Xia Q, Wei DSL, Yue H, Wu F. A secure, efficient, and accountable edge-based access control framework for information centric networks. IEEE/ACM Trans Networking 2019;27(3):1220–33. doi: https://doi.org/10.1109/TNET.2019.2914189.
[11] Wenting Li, Ping Wang, Cryptanalysis of Two Chaotic Maps-based Authentication Schemes in Edge Computing, 5th IEEE International Conference on Edge Computing and Scalable Cloud, Paris, France, 2019. doi: 10.1109/CSCloud/EdgeCom.2019.000-2.
[12] Omar AA, Bhuiyan MZA, Basu A, Kiyomoto S, Rahman MS. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Generation Computer Systems 2019;95:511–21. doi: https://doi.org/10.1016/j.future.2018.12.044.
[13] Brunese L, Mercaldo F, Reginelli A, Santone A. A blockchain based proposal for protecting healthcare systems through formal methods. Procedia Comput Sci 2019;159:1787–94. doi: https://doi.org/10.1016/j.procs.2019.09.350.
[14] Chen L, Lee W-K, Chang C-C, Choo K-K, Zhang N. Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems 2019;95:420–9. doi: https://doi.org/10.1016/j.future.2019.01.018.
[15] Malathi D, Logesh R, Subramaniyaswamy V, Vijayakumar V, Sangaiah Arun Kumar. Hybrid reasoning-based privacy-aware disease prediction support system. Comput Electr Eng 2019;73:114–27. doi: https://doi.org/10.1016/j.compeleceng.2018.11.009.
[16] Kruthika KR, Rajeswari HD, Maheshappa, Multistage classifier-based approach for Alzheimer's disease prediction and retrieval, Informatics in Medicine Unlocked, vol. 14, pp. 34–42, 2019. doi: 10.1016/j.imu.2018.12.003.
[17] Yakubu Jimoh, Abdulhamid Shafi'i Muhammad, Christopher Haruna Atabo, Chiroma Haruna, Abdullahi Mohammed. Security challenges in fog-computing environment: a systematic appraisal of current developments. J Reliable Intell Environ 2019;5(4):209–33. doi: https://doi.org/10.1007/s40860-019-00081-2.
[18] Qiu Han, Qiu Meikang, Lu Zhihui. Selective encryption on ECG data in body sensor network based on supervised machine learning. Information Fusion 2020;55:59–67. doi: https://doi.org/10.1016/j.inffus.2019.07.012.
[19] Patonico Simone, Braeken An, Steenhaut Kris. Identity-based and anonymous key agreement protocol for fog computing resistant in the Canetti-Krawczyk security model. Wireless Netw 2019. doi: https://doi.org/10.1007/s11276-019-02084-6.
[20] Zhou Tianqi, Shen Jian, Li. Xiong, Wang Chen, Tan Haowen. Logarithmic encryption scheme for cyber–physical systems employing Fibonacci Q-matrix. Future Generation Computer Systems 2020;108:1307–13. doi: https://doi.org/10.1016/j.future.2018.04.008.
[21] Liu Yuxin, Liu Xiao, Liu Anfeng, Xiong Neal N, Liu Fang. A trust computing-based security routing scheme for cyber physical systems. ACM Trans Intell Syst Technol 2019;10(6):1–27. doi: https://doi.org/10.1145/3321694.
[22] Ma Mimi, He Debiao, Fan Shuqin, Feng Dengguo. Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare. J Information Security Appl 2020;50:102429. doi: https://doi.org/10.1016/j.jisa.2019.102429.
[23] Tahir Shahzaib, Ruj Sushmita, Sajjad Ali, Rajarajan Muttukrishnan. Fuzzy keywords enabled ranked searchable encryption scheme for a public Cloud environment. Comput Commun 2019;133:102–14. doi: https://doi.org/10.1016/j.comcom.2018.08.004.
[24] Zhou Yousheng, Zhao Xiaofeng, Liu Siling, Long Xingwang, Luo Wenjun. A time-aware searchable encryption scheme for EHRs. Digital Commun Networks 2019;5(3):170–5. doi: https://doi.org/10.1016/j.dcan.2018.09.003.
[25] Alabdulatif Abdulatif, Kumarage Heshan, Khalil Ibrahim, Yi Xun. Privacy-preserving anomaly detection in cloud with a lightweight homomorphic approach. J Comput Syst Sci 2017. doi: https://doi.org/10.1016/j.jcss.2017.03.001.
[26] Alloghani Mohamed, M. Alani Mohammed, Al-Jumeily Dhiya, Baker Thar, Mustafina Jamila, Hussain Abir, J. Aljaaf Ahmed. A systematic review on the status and progress of homomorphic encryption technologies. J Information Security Appl 2019;48:102362. doi: https://doi.org/10.1016/j.jisa.2019.102362.
[27] Sun Pan Jun. Security and privacy protection in cloud computing: discussions and challenges. J Network Comput Applications 2020;160:102642. doi: https://doi.org/10.1016/j.jnca.2020.102642.
[28] Abd EL-Latif Ahmed A, Abd-El-Atty Bassem, Abou-Nassar Eman M, Venegas-Andraca Salvador E. Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things. Opt Laser Technol 2020;124:105942. doi: https://doi.org/10.1016/j.optlastec.2019.105942.
[29] Hassan Abdelrhman, Wang Yong, Elhabob Rashad, Eltayieb Nabeil, Li Fagen. An efficient certificateless public key encryption scheme with authorized equality test in healthcare environments. J Syst Archit 2020;109:101776. doi: https://doi.org/10.1016/j.sysarc.2020.101776.
[30] Hameed Mustafa Emad, Ibrahim Masrullizam Mat, Manap Nurulfajar Abd, Mohammed Ali A. A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES. Future Generation Computer Systems 2020;111:829–40. doi: https://doi.org/10.1016/j.future.2019.10.010.
[31] He Qian, Zhang Ning, Wei Yongzhuang, Zhang Yan. Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems. Comput Netw 2018;140(20):163–73. doi: https://doi.org/10.1016/j.comnet.2018.01.038.
[32] Wu Libing, Zhang Yubo, Choo Kim-Kwang Raymond, He Debiao. Efficient and secure identity-based encryption scheme with equality test in cloud computing. Future Generation Computer Systems 2017;73:22–31. doi: https://doi.org/10.1016/j.future.2017.03.007.
[33] Geetha R, Suntheya AK, Umarani Srikanth G. Cloud integrated IoT enabled sensor network security: research issues and solutions. Wireless Personal Commun 2020. doi: https://doi.org/10.1007/s11277- 020-07251-z.
[34] Prashanth R, Dutta Roy Sumantra, Mandal Pravat K, Ghosh Shantanu. High-accuracy detection of early Parkinson's disease through multimodal features and machine learning. Int J Med Inf 2016;90:13–21. doi: https://doi.org/10.1016/j.ijmedinf.2016.03.001.
[35] Ayyad Sarah M, Saleh Ahmed I, Labib Labib M. Gene expression cancer classification using modified K-Nearest Neighbors technique. Biosystems 2019;176:41–51. doi: https://doi.org/10.1016/j.biosystems.2018.12.009.
[36] Chen Hui-Ling, Huang Chang-Cheng, Yu Xin-Gang, Xu Xin, Sun Xin, Wang Gang, Wang Su-Jing. An efficient diagnosis system for detection of Parkinson's disease using fuzzy k-nearest neighbor approach. Expert Syst Appl 2013;40(1):263–71. doi: https://doi.org/10.1016/j.eswa.2012.07.014.
[37] Gou Jianping, Ma Hongxing, Ou Weihua, Zeng Shaoning, Rao Yunbo, Yang Hebiao. A generalized mean distance-based k-nearest neighbor classifier. Expert Syst Appl 2019;115:356–72. doi: https://doi.org/10.1016/j.eswa.2018.08.021.
[38] Mamun Khondaker Abdullah Al, Alhussein Musaed, Sailunaz Kashfia, Islam Mohammad Saiful. Cloud based framework for Parkinson's disease diagnosis and monitoring system for remote healthcare applications. Future Generation Computer Systems 2017;66:36–47. doi: https://doi.org/10.1016/j.future.2015.11.010.
[39] Azimi Iman, Anzanpour Arman, Rahmani Amir M, Pahikkala Tapio, Levorato Marco, Liljeberg Pasi, Dutt Nikil. HiCH: Hierarchical Fog-Assisted Computing Architecture for Healthcare IoT. ACM Trans Embed Comput Syst 2017;16(5s):1–20. doi: https://doi.org/10.1145/3126501.
[40] Kharel Jeevan, Reda Haftu T, Shin Soo Y. An architecture for smart health monitoring system based on fog computing. J Commun 2017. doi: https://doi.org/10.12720/jcm.12.4.228-233.
[41] Soraia Oueida, Yehia Kotb, Moayad Aloqaily, Yaser Jararweh, Thar Baker, An edge computing based smart healthcare framework for resource management, Sensors, vol. 18, Article 4307, 2018. doi: 10.3390/s18124307.
[42] Tshiamo Sigwele, Yim Fun Hu, Muhammad Ali, Jiachen Hou, Misfa Susanto, Helmy Fitriawan, An Intelligent Edge Computing based Semantic Gateway for Healthcare Systems Interoperability and Collaboration, IEEE 6th International Conference on Future Internet of Things and Cloud, Barcelona, Spain, 6-8 Aug 2018.
[43] Little MA, McSharry PE, Roberts SJ, Costello DAE, Moroz IM. Exploiting nonlinear recurrence and fractal scaling properties for voice disorder detection. Bio Medical Eng. 2007;6:1–19. doi: https://doi.org/10.1186/1475-925X-6-23.
[44] Oxford Parkinson's Disease Detection Dataset, 2008. Parkinsons Data Set, UCI Machine Learning Repository. http://archive.ics.uci.edu/ml/datasets/parkinsons. Accessed on 8 April 2020.
[45] Sun Yi, Wen Qiaoyan, Zhang Yudong, Li Wenmin. Privacy-preserving self-helped medical diagnosis scheme based on secure two-party computation in wireless sensor networks. Comput Math Methods Med 2014;2014:1–9. doi: https://doi.org/10.1155/2014/214841.
[46] Guo Wei, Shao Jun, Lu Rongxing, Liu Yining, Ghorbani Ali A. A privacy-preserving online medical prediagnosis scheme for cloud environment. IEEE Access 2018;6:48946–57. doi: https://doi.org/10.1109/ACCESS.2018.2866971.
[47] Wang Chengjia, Dong Shizhou, Zhao Xiaofeng, Papanastasiou Giorgos, Zhang Heye, Yang Guang. SaliencyGAN: Deep Learning Semisupervised Salient Object Detection in the Fog of IoT. IEEE Trans. Ind. Inf. 2020;16(4):2667–76. doi: https://doi.org/10.1109/TII.2019.2945362.