[Egyptian Informatics Journal 22 (2021) 401–410](https://doi.org/10.1016/j.eij.2020.12.003)

Contents lists available at [ScienceDirect](http://www.sciencedirect.com/science/journal/11108665)

Egyptian Informatics Journal

journal homepage: [www.sciencedirect.com](http://www.sciencedirect.com/)

[](http://crossmark.crossref.org/dialog/?doi=10.1016/j.eij.2020.12.003&domain=pdf)Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system

Ramaprabha Jayaram [⇑](#_bookmark0), S. Prabakaran

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

a r t i c l e i n f o

*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

a b s t r a c t

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 diag- nosis through various prediction processes made by the decision support system. These sensing and pro- cessing 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 pro- posed 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.

© 2021 THE AUTHORS. Published by Elsevier BV. on behalf of Faculty of Computers and Artificial Intel-

ligence, Cairo University. This is an open access article under the CC BY-NC-ND license ([http://creative-](http://creativecommons.org/licenses/by-nc-nd/4.0/)

[commons.org/licenses/by-nc-nd/4.0/](http://creativecommons.org/licenses/by-nc-nd/4.0/)).

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 repos- itories [[1]](#_bookmark29). 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]](#_bookmark30). 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

\* Corresponding author.

*E-mail address:* [ramaprabhajayaram@gmail.com](mailto:ramaprabhajayaram@gmail.com) (R. Jayaram).

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

uploaded by multiple users which may be accidentally disclosed [[3]](#_bookmark31). This situation will open the door of prying eyes to launch var- ious levels of security attacks such as data privacy, integrity and confidentiality in healthcare systems. To provide security, an attri- bute 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]](#_bookmark32). Now-a-days, the edge-based healthcare services were employed for cost effec- tive data processing and network resource provisioning on edge computing framework through data offloading and real-time pro- cessing respectively. Here, computational offloading at edge level can minimize the energy consumption, communication and com- putational delay between edge and cloud server [[5]](#_bookmark33). Existing healthcare system research was focused more on data processing and data sharing security mechanisms at cloud server level [[6,7]](#_bookmark34). 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,

<https://doi.org/10.1016/j.eij.2020.12.003>

1110-8665/© 2021 THE AUTHORS. Published by Elsevier BV. on behalf of Faculty of Computers and Artificial Intelligence, Cairo University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

there might be some inevitable cause leads to security issues like users privacy and providers business value [[8]](#_bookmark35). 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 com- puting platform. More specifically some security threats like side channel attacks, virtualization vulnerabilities, networks eaves- dropping and denial of service attacks are tightly associated with cloud data service [[9]](#_bookmark35). 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 sig- nal 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 encryp- tion 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 proba- bilistic classifier model in the cloud level for onboard disease pre- diction 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]](#_bookmark35). A chaotic maps-based authentication scheme is employed in the edge computing level to realize the two factor data security and forward secrecy [[11]](#_bookmark35). 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]](#_bookmark35). In addition, block- chain 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]](#_bookmark35). 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 effec- tiveness data processing transaction overhead on real-time smart contracts exploited in the healthcare system [[14]](#_bookmark35).

Apart from security, proposed research includes the implemen- tation of adaptive classifier models in the edge-cloud-based healthcare system. Existing healthcare system exploited the reasoning-based privacy-aware decision support system for dis- ease prediction and preservation of patient sensitive data [[15]](#_bookmark35). 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 dis- ease [[16]](#_bookmark36). 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 monitor- ing 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](#_bookmark2), provides a detailed description of proposed edge-cloud-based healthcare system architecture with appropriate security and classifier model. In sec-

tion 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.

1. Related works
   1. *Security in cloud based smart healthcare system*

According to recent research studies in healthcare systems, var- ious security mechanisms were adopted in both edge and cloud level as given in [Fig. 1](#_bookmark1). At edge level, security techniques are applied in the context of cryptography, machine learning and com- putational intelligence approach [[17]](#_bookmark37). Here, the cryptography approach includes the advanced encryption standard, secure sock- ets 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]](#_bookmark38). 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]](#_bookmark43). 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]](#_bookmark45). To establish secure rout- ing 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]](#_bookmark47).

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]](#_bookmark48). 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]](#_bookmark50). 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 pro- vide more security and efficiency than the existing schemes [[24]](#_bookmark53). A homomorphic encryption scheme was introduced to manage large-scale sensor data with high level privacy preserving anom- aly detection service in cloud-based electronic health records [[25]](#_bookmark54). 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]](#_bookmark56). According to literature study, some prominent schemes such as key policy attribute-based encryption, trust, multi-tenant, multi-authority, fine-grain, revo- cation mechanism, trace mechanism, proxy re-encryption and hierarchical encryption were analyzed for ensuring security and privacy in cloud [[27]](#_bookmark58).

Next, a quantum walks-based encryption was composed of sub- stitution and permutation phases in healthcare systems for pro- tecting the patients’ privacy without compromising the robustness and efficiency of image encryption [[28]](#_bookmark60). An authorized cloud server was protected with novel certificate less public-key

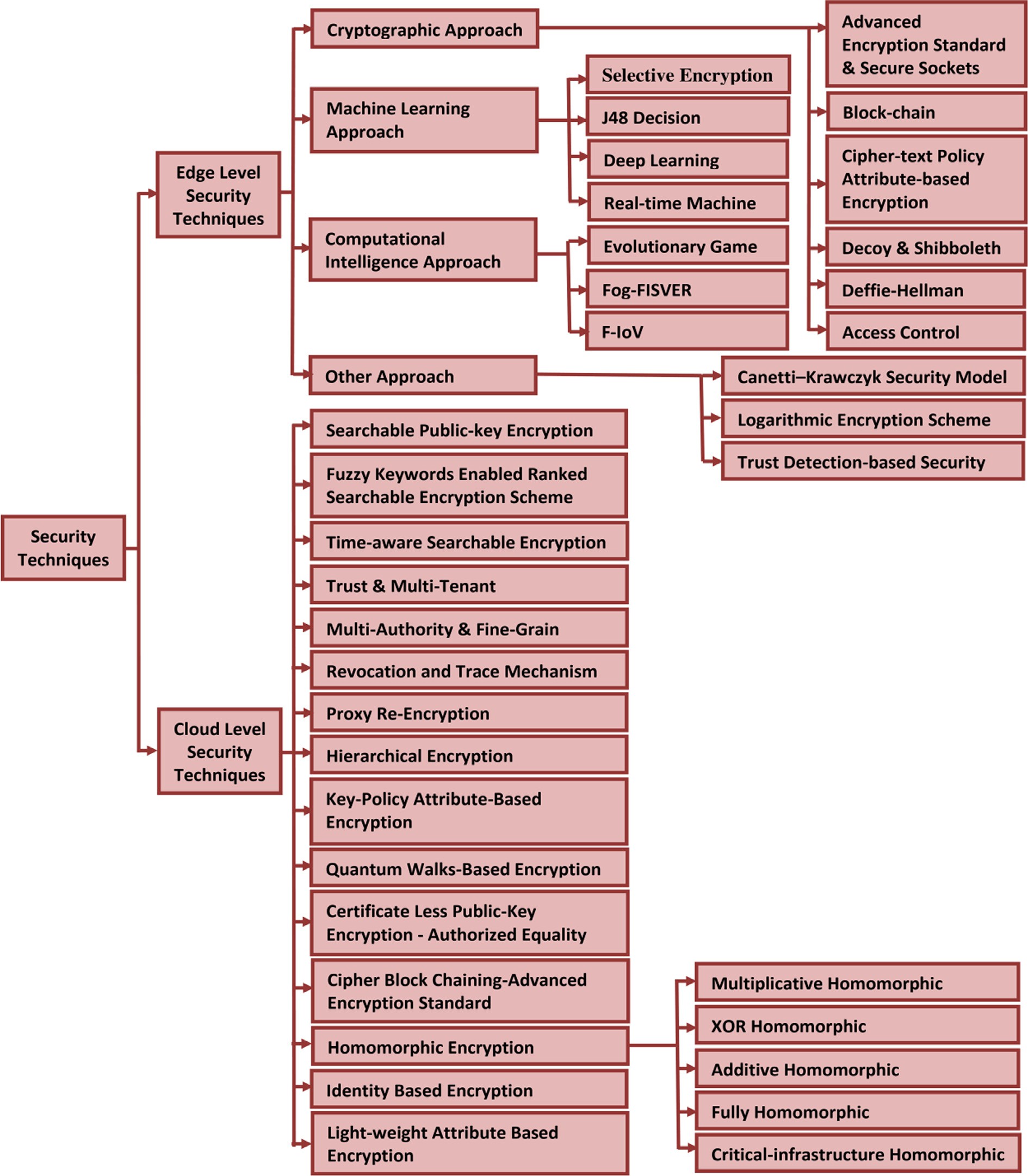


Fig. 1. Taxonomy of security techniques.

encryption along with authorized equality test scheme before out- sourcing to smart healthcare service [[29]](#_bookmark39). 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]](#_bookmark39). 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]](#_bookmark39). 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]](#_bookmark39). 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 ser- vice, phishing, flooding request, malware injection and target shared memory attacks involved in both edge and cloud environ- ment [[33]](#_bookmark39). Therefore, the proposed research focuses on privacy preserving additive homomorphic encryption development to ensure secure data transfer and offloading computation at edge level.

* 1. *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 plat- forms. 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]](#_bookmark39). As a result, kernel-based support vector machine clas- sifiers 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]](#_bookmark39). A fuzzy based k-NN classifier model was proposed to design an efficient diagnosis system for improving the perfor- mance of Parkinson disease detection [[36]](#_bookmark40). Sometimes, the sensi- tivity of the k value may degrade the performance of the classifier in case of less sample size with traditional outliers. There- fore, a generalized mean distance-based k-NN classifier model was employed by estimating categorical nested and multi-generalized mean distances [[37]](#_bookmark41). 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 train- ing 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.

* 1. *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](#_bookmark3). A cloud-based framework is designed with two layer healthcare architecture for Parkinson disease monitoring and diag- nosis from remote place [[38]](#_bookmark42). Next, a hierarchical fog-assisted computing architecture is designed with three layers for enhancing IoT based healthcare application [[39]](#_bookmark44). Similarly, a fog based smart healthcare monitoring is presented with three layers for monitor- ing the human body vital signals like heart rate, respiratory rate, stress, temperature and pressure level [[40]](#_bookmark46). 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]](#_bookmark49). In order to pro- vide interoperability among the healthcare systems, a semantic based healthcare interoperability framework is explored to provide secure information exchange [[42]](#_bookmark51). While comparing the architec- ture of all the healthcare systems, the proposed secure edge- cloud-based healthcare system provides better security, interoper- ability and performance measurement attributes.

1. 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](#_bookmark4). 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 preserv- ing additive homomorphic encryption is proposed to protect the sensitive data against the attackers. In edge level, the proposed architecture incorporates a microcontroller device called Rasp- berry Pi complete kit to enforce security and data offloading mech- anism. 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 plat- forms. 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 | Prediction Time, Prediction Accuracy |
| Hierarchical fog-assisted computing | Sensor, Fog, Cloud | No Security | Interoperability  No | Response Time, Capacity Utilization, Quick Data |
| architecture  Fog-based smart healthcare monitoring | IoT, Fog, Cloud | No Security | Interoperability  No | Access  Quick Data Access |
| Edge computing based smart healthcare | User, Fog/Edge, Cloud | Data Accessibility | Interoperability  No | Length of Stay, Resource Utilization, Patient |
| framework  Semantic based healthcare | Smart-Device, Fog, | Base Level Data Security | Interoperability  Interoperability | Waiting Time  Restful Protocol |
| interoperability framework  Fog computing based preventive | Cloud  Interaction, Mesh, | Trust based Security | No | Interoperability |
| healthcare  Proposed secure edge-cloud-based | Fog, Cloud  Sensor, Edge, Cloud | Additive Homomorphic | Interoperability  Interoperability | Prediction Time, Prediction Accuracy, Response |
| healthcare system |  | Encryption |  | Time, Capacity Usage |

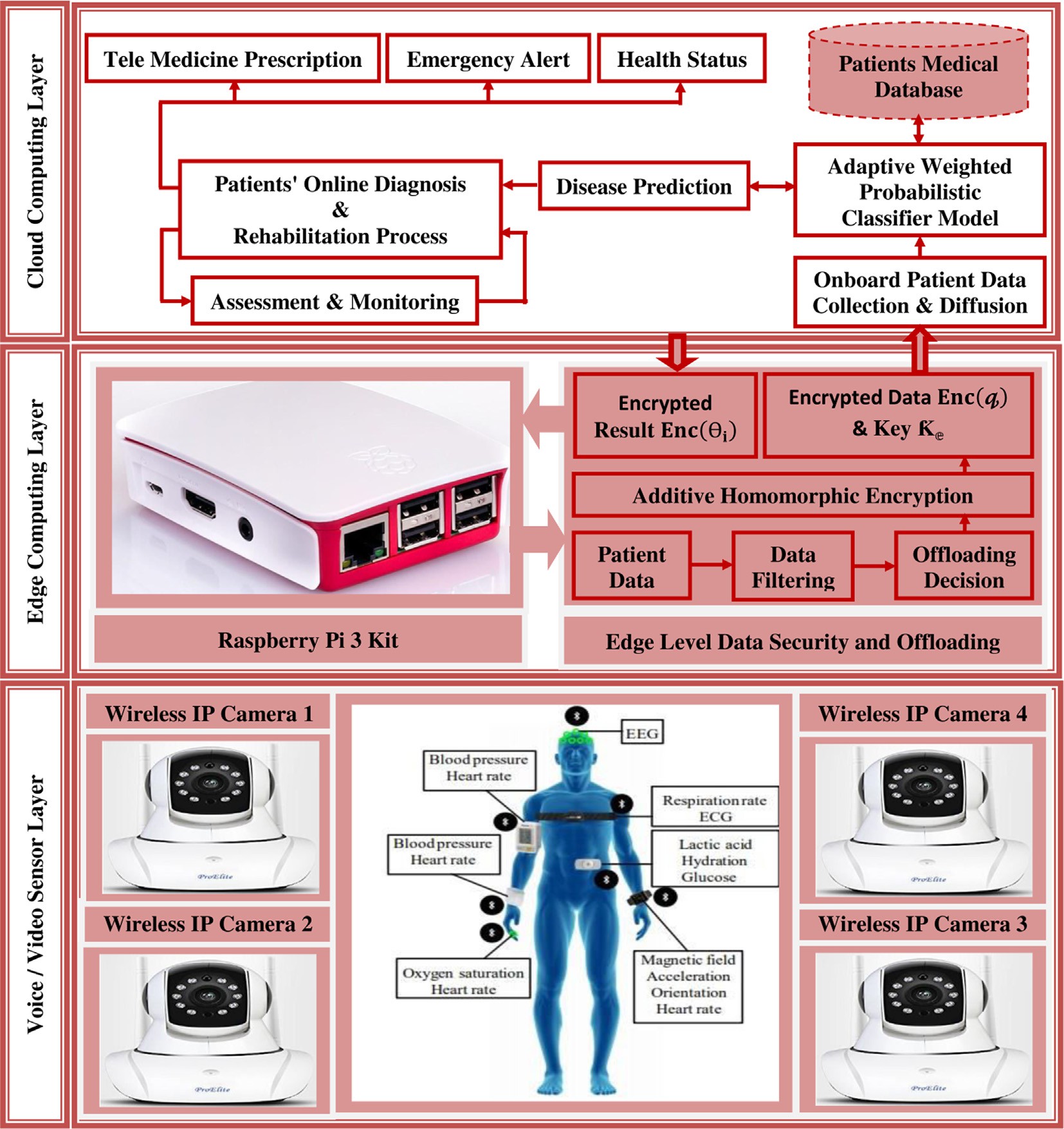


Fig. 2. Secure Edge-Cloud-based Healthcare System Architecture.

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 reha- bilitation 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 subscrip- tion and predefined health policy activated by the remote patient.

* 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 fil-

tering scheme is adopted to filter all the non-sensitive data in the edge node and offload only the sensitive data to cloud comput- ing nodes available in the *CLayer*. Therefore, the offloading problem can be defined with *n* number of edge computing nodes

*EN* = {*EN*1; *EN*2; ··· ; *ENn*} as shown in equation [(1)](#_bookmark5). Then, the min- imization of offloading function Z(*EN*) is described in equation [(2)](#_bookmark6) with constraints such as *n ENi* = *DO*, *ENi* ≤ SLA*i* and *ENi* ≥ 0. Let SLA*i* be the service level agreement parameter be enforced

*i*=1

P

on edge nodes and *DO* be the total amount of patient data tasks need to be offloaded to cloud computing nodes available in *CLayer*

i.e., *DO* = *VP* .

*Total*

*MinEN*Z(*EN*) (1)

X

*n*

Z(*EN*) = *x* \* T *off* (*ENi*) + (1 — *x*) \* *eoff* (*ENi*) (2)

*i*=1

where *x* be the weighting parameter of offloading transmission

time and energy consumption, T *off* be the offload transmission time and *eoff* be the offload energy consumption of edge node *ENi* during offloading activity. Here, the offload transmission time at any time

stamp *s* can be measured based on the size of computable input data *V* ¡ and uplink data rate R*UpLink* as given in equation [(3)](#_bookmark7).

*V* ¡*s*

respective medical data *V* = {*V* 1; *V* 2; ·· · ; *Vn*}. This query vector includes the necessary features of disease diagnosis and also needs

to be clearly determined by the trait vector of the healthcare sys-

T *off* (*ENi*) =

R*UpLink*

*s* (3)

tem. Then the cloud layer will present the medical database

*D*^ = {*D*^ 1; *D*^ 2; ··· ; *D*^ *n* } of patients as quadruple as given in equation

Similarly, the offload energy consumption at edge node *ENi* can be measured as formulated in equation [(4)](#_bookmark7). Let *eTail* denote the tail energy to hold the communication channel even after data trans-

mission and PT denote the offload transmission power of edge nodes *ENi*.

*s*

*off* ( *i*) = ¡ + *Tail* ( )

*s*

*e EN*  PT *V e* 4

R*UpLink*

In order to satisfy the committed SLA*i* at *CLayer*, the total energy consumption and network delay of correspond cloud node should be minimized for improve the response time of proposed health- care system. This improvement can be made possible by minimiz- ing the delay and network capacity incurred by edge level offloading process. Accordingly, estimate the allocation of network capacity between *ENi* and cloud nodes *CNj* by using equation [(5)](#_bookmark8).

[(9)](#_bookmark9), based on the sequence of previously sensed medical data.

*D*^ *i* = I*i*; *Ci*; *Ti*; H*i* (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 diagno- sis and rehabilitation of disease, b*i* denotes the final diagnostic out-

put of healthcare system which includes disease name, clinical manifestation and doctor prescriptions related to disease D*i*.

T*i* = (t*i*1; t*i*2; ··· ; t*in*) of disease repository for identifying the devia- The healthcare system in *CLayer* will maintain the trait vectors tion 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 repos- itory. In order to identify the deviation of medical features between

the trait vectors of patient query *q* and disease repository D*i*, an

*bENi* —*CNj*

*bENi* (*pENi* )

= *pEN*

*i*

(5)

Euclidean distance is measured as shown in equation [(10)](#_bookmark10).

*d*(*q*; D*i*) =  *q* — D*i * 2 (10)

where *pENi* be the offloading capacity of edge nodes *ENi*∈(1;*n*), and

*bENi* (*pENi* ) represents the amount of network capacity among the

Due to the expansion of distance parameter evaluation such as

*q* — D2 = (*q* — *t* )2 + (*q* — t )2 + ... + (*q* — t )2, the equation [(10)](#_bookmark10)

edge nodes shared by the corresponding cloud node *CNj*. The total

*i* 1 *i*1

2 *i*2

*n in*

delay D to serve the patient data offloading request at time period

*s* can be formulated as shown in equation [(6)](#_bookmark12). Here, the binary vari-

can be rewritten as equation [(11)](#_bookmark11).

*n n n*

*s d*(*q*; D*i*) = X *q*2 + X t2 + X —2*qj* t*ij* (11)

*CNj*

able *uVi* should be used to characterize whether the cloud node *CNj*

can serve the data request of the edge node *ENi* or not.

*j*=1

*j*

*j*=1

*ij*

*j*=1

*s*

D

*Total*

*s*

*ENi* —*CNj*

= D

*s*

*ENi* —*CNj*

+ Q

*s*

*CNj*

*u*

*s*

*ENi* —*CNj*

+ Q

(1 — *us*

## ) (6)

Then, the complete similarity between the trait vectors of patient query *q* and disease repository D*i* is formulated as shown

However, the delay incurred to transfer patient medical data from edge node *ENi* to cloud node *CNj* can be computed as given in equation [(7)](#_bookmark14).

in equation [(12)](#_bookmark13).

*Sim*(*q*; D*i*) = 1

1 + *d*(*q*; D*i*)

## (12)

*s*

D

*ENi* —*CNj*

*s*

= *Vi* +

*d*

*bEN*

*s*

*ENi*

*d*

*ps*

—*CNj*

(7)

Here, the similarity range [0,1] denotes the distance closer where higher similarity value indicated less deviations in trait vec-

*i*—*CNj*

*ENi* —*CNj*

tors of patient (less improvements on diagnosis) and smaller simi-

Let *ds*

*Vi*

be the size of patient medical data request to be pro-

larity value indicated more significant deviations in trait vectors of

cessed in time slot *s*, *ds*

*ENi* —*CNj*

be the strength of signal decay

patient (more improvements on diagnosis). According to deviation

between edge node *ENi* and cloud node *CNj*, and *ps*

*ENi* —*CNj*

be the

in similarity value, the doctor will change the diagnosis and rehabil-

itation process until there are some improvements observed from

propagation speed of communication medium established between *ENi* and *CNj*. Next, the queuing delay in the cloud node *CNj* to process the patient data request received from edge nodes *ENi* can be estimated using equation [(8)](#_bookmark15).

the trait vectors of patient data during subsequent monitoring states.

In order to maintain the patient’s privacy, an additive homomor- phic encryption scheme is employed to encrypt the trait vectors of

*s*

*ENi* —*CNj*

Q

*s*

*CNj*

= T

1

— *s*

*l*

*CNj*

(8)

as *Enc*(*q*) and *Enc*(T*i*) respectively. Therefore, first generates the key patient data and disease repository data from edge and cloud layer

pairs (K ; K ) for initiating the additive homomorphic encryption

e d

where T *s*

*CNj*

denotes the average amount of time spent by patient

over the trait vectors of patient data. Then, the healthcare system

data in cloud node *CNj*, and *ls* denotes the number of patient data

*CNj*

uses the encryption key Ke to encrypt the patient data query *q* as

*Enc*(*q*) = (*Enc*(*q* ); *Enc*(*q* ); ··· ; *Enc*(*q* )). Finally, the edge node will

request served in cloud node *CNj* at time slot *s*.

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

After data filtering at edge nodes, offloading decisions will initi- ate the privacy preserving cryptosystem to ensure the privacy and security during the offloading of patient data from edge node to

1 2 *n*

send the cipher text of patient data C*i* = *Enc*(*q*) along with the encryption key Ke to the cloud layer. Afterwards, the healthcare sys-

tem will perform the homomorphic encryption computation given

itory T*i* and the cipher text *Enc*(*q*) received from the patient with in equation [(13) and (14)](#_bookmark16) based on the trait vectors of disease repos- corresponding encryption key Ke.

*M* = *Enc* X*n* t 2 (13)

cloud node. Therefore, the sequence of past and present medical 2

data sensed from patient’s are periodically encrypted and offloaded

3

*j ij*

*j*=1

*j*

*j*=1 *ij*

to cloud node available at *CLayer*. Assume the patients query vector

*j*=1

1

2

*n*

*q* = {*q* ; *q* ; ··· ; *q* } denotes the set of patients query with their

*M* = *Enc* X*n*

(—2*q* t ) = P*n*

*Enc* *q* —2t*ij* (14)

vacy information of cipher text *Enc*(*q*), a set of random numbers To further prevent other stakeholders from obtaining the pri- H = {*h*1; *h*2; ··· ; *hn*}. These random numbers of H will make some are generated by the patient to form n-dimensional vector as disturb in the information of *q*. Then, the patient will be computed

samples *Sk*∈(1;*n*) applied through joint distribution of total data ser- expected value constraints. It can be formulated using the set of vice request and *VM* availability as given in equation [(19)](#_bookmark18).

*n*

1 X

C*Total*(*Vi*) + *p* \* *VP* (*Sk*) — *VVM* (*Sk*) (19)

*Total*

*Total*

s = *Enc* P*n aj* 2 and sent to the healthcare system for getting fur-

*j*=1

*n k*=1

*aj* = *qj* + *hj*. At last, the healthcare system computes the M1 as ther diagnosis and rehabilitation from the doctor where shown in equation [(15)](#_bookmark17). Then, the encrypted distance measure

*Enc*(D ) is computed as given in equation [(16)](#_bookmark17) and sent to the

Thus, the above sample average approximation solution of opti- mization problem can redefine the objective function of [(18)](#_bookmark23) as shown in equation [(20)](#_bookmark18). The corresponding constraints are defined

as *Vi* ≥ *VMin*, *Vi* ≤ *VMax* and *VVM* ≤ *VP* . Due to sample selection

*i i* *i*

*Total*

*Total*

patient.

this solution may arrive at a near optimal result. Therefore, the val-

*P VM*

*M* = s · P*n*  *Enc* —2*hj* · *Enc* — = *Enc* X*n*  (15)

*k*∈(1;*n*)

1

*qj*

*j*=1*qj*

validity with respect to the total validation sample *SVal*

. As a

*h*2 2

*j*=1

*j*

idation set (*V*b *Total* ; *V*b *Total* ) is exercised to test the optimal solution

*Enc*(D*i*) = *M*1 · *M*2 · *M*3 (16)

result, the validity checking optimization solution of sample aver- age approximation can be defined as given in equation [(21)](#_bookmark19) with

*VM P*

b b

After substituting the value of M1, M2 and M3 in equation [(16)](#_bookmark17), the summative encryption is obtained as composed in equation

*Total*

respect to constraint *V Total* ≤ *V Total* .

# " 1 X #

*n*

[(17)](#_bookmark17).

*Enc*(D ) = *Enc* X*n*

*i*

*j*=1

*q* 2 + X*n*

t 2 + X*n*

(—2*q* t ) (17)

*Minimize* C*Total*(*Vi*) + *n*

*k*=1

*P*

*Total*

*p* \* *V*

(*Sk*) — *VVM* (*Sk*)

## (20)

After estimating encrypted distance measure D

*j*

*j*=1 *ij*

*j*=1

*j ij*

(

*i*)

, the health-

# " 1 X

b *P*

*Val*

b *VM* *Val* #

care system will decrypt *Enc*(D*i*) as D*i* and compute the similarity

function *Sim q*; 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 health-

care system through proper encryption *Enc*(H*i*) with the respective

patients. Finally, the remote patient can decrypt the obtained

*k*=1

The equivalent certainty of sample average approximation solu-

*n*

*Minimize* C*Total*(*Vi*) + *n*

*p* \*

*V Total Sk*

— *V Total Sk*

(21)

tion can be formulated as given in equation [(22)](#_bookmark20). Similarly, the validity checking of equivalent certainty solutions can be derived with the same constraints as given in equation [(23)](#_bookmark21) using the opti- mization approach.

*Total*

result H*i* to undergo further diagnosis and rehabilitation process given by the doctor.

*Minimize*hC*Total*(*Vi*) + *p* \* *Max* 0; *Average* *VP*

*VM*

*Total*

— *Average*(*V* ) i

(22)

*Total*

*i*

*Total*

*Total*

(23)

* 1. *Disease prediction and rehabilitation in healthcare system using*

*adaptive weighted probabilistic classifier model*

*Minimize*hC (*V* ) + *p* \* *Max* 0; *Average* *V*b *P* — *Average*(*V*b *VM* ) i

The healthcare service provisioning from cloud layer has effec- tive storage and processing capability for real-time disease predic- tion and rehabilitation process by exploiting the proposed adaptive weighted probabilistic classifier model. After receiving the

patient’s data requests from various geographic regions, the pro-

At any time stamp D*s*, the proposed healthcare system can pre- dict the disease severity of patient data *Vi* during the state of reha- bilitation assessment and monitoring activity as formulated in equation [(24)](#_bookmark22).

posed classifier will be exploited by the healthcare system for quick prediction and response generation to concern. At cloud

*k*=1

*k*

D*s*

*Disease*

*P*

(*Vi*)= *Max*P*L*

*P* F *s*|*SI*F (24)

layer *CLayer*, there are *n* number of live data request *Vi*∈(1;*n*) were received to process in the classifier service which in turn paral-

*VMj*∈(1;*m*). A classifier service hosted at each *VM* can have a maxi- lelize the data processing task to *m* number of virtual machines mum *VMMax* and minimum *VMMin* bound of data processing capa-

*DP DP*

bility for processing the corresponding maximum *VMax* and

*i*

minimum *VMin* amount of data tasks respectively. Now, the objec- tive of research is to minimize the cost of *VM* provisioning initiated for data processing at classifier service hosted in *CLayer* as defined in equation [(18)](#_bookmark23).

*i*

*Minimize* C*Total*(*Vi*) + *E*h*p* *VP* — *VVM* i (18)

*Total*

*Total*

Let C*Total* represents the total cost of processing data task *Vi*∈(1;*n*),

*Total*

*VP* denotes the total data service demanded by the remote

all possible *VMj*∈(1;*m*) at time *s*. Finally, *E p VP* — *VVM* repre- patients and *VVM* denotes the overall data service obtainable from sents the expected cost of buying healthcare service from *CLayer*

*Total*

*Total*

*Total*

h i

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

Let *L* denotes the length of time spent by the patient data on cloud layer during prediction, F *s* denotes the observed character- istic feature of disease at time *s*, and *SI*F be the severity indicator

of feature assessed during rehabilitation process. The positive

*k*

under the observed feature F are given as *P*(F|S+) and *P*(F|S—) and negative probability value of experiencing the disease severity with respect to threshold value U. Next, the weighted prior proba-

bility of feature F at time stamp D*s* can be measured as defined in equation [(25)](#_bookmark24).

*P*D*s*(F|S+) = *P* F *T* \* *P* F *T* |S+ (25)

*W*

the value as defined in equation [(26) and (27)](#_bookmark25). Let *W*(F *s*) repre- Similarly, the weighted posterior probability function can infer sents 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*D*s*(S+|F) = *PW* (F *s*|S+) \* *P*(S+)*P*(F *s*) (26)

*W*

## *P*D*s*(S+|F) = *W*(F *s*)\* *P*(F *s*|S+) \* *P*(S+)*P*(F *s*) (27)

*W*

Here, the value of *P*(F *s*) can be expressed as given in equation

[(28) and (29)](#_bookmark26).

*P*(F *s*) = *PW* (F *s*|S+)*P*(S+) + *P*(F *s*|S—)*P*(S—) (28)

## *P*(F *s*) = *W*(F *s*)*P*(F *s*|S+)*P*(S+) + *P*(F *s*|S—)*P*(S—) (29)

Finally, the severity indicator value *SI*D*s* is estimated as formu-

F

lated in equation [(30)](#_bookmark26) based on the number of features observed from the patient data during time stamp D*s*. Therefore, the aggre- gated heterogeneous activity of patient data *Vi* is formulated for disease severity identification as given in equation [(31)](#_bookmark26).

D*s* 1 D*s*

*SI* = X *P* (S |F) (30)

F *W* +

*k*

F

time, prediction time and prediction accuracy. Initially, the classi- fier is trained with two benchmarking voice dataset taken from University of California-Irvine (UCI) repository [[43,44]](#_bookmark52). The train- ing dataset has sound recordings of 195 voice samples, out of which 147 samples affected and 48 samples not affected by Parkin- son 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.

*P*D*s* (*Vi*) = *Argmaxk* 1 2 *LP* *SI*D*s* P*L* 1*P* F *s*|*SI*F (31)

*Disease*

= ; ;···;

F

*k*=

*k*

Prediction Accuracy *PAccuracy* can be defined by the ratio of prop- erly classified incidence to the total presented incidence as given in equation [(32)](#_bookmark26).

*Disease*

*4.2. Results and discussion*

The proposed SECHS performance is measured by comparing with existing healthcare systems such as Smart Architecture for

*Accuracy*

*T*+ + *T*—

in Home Healthcare (SAHH) and IoT-based Healthcare Smart

*PDisease* = *T*+ + *F*+ + *T*— + *F*— (32)

Where *T*+, *T*—, *F*+ and *F*— represents the quantity of true posi- tives, true negatives, false positives and false negatives respec-

tively. 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 reha- bilitation monitoring service for each patient. Then, the patient can

decrypt and follow the diagnosis and rehabilitation methods b*i*

suggested by the doctor. Also the system will periodically monitor and assess the disease diagnosis and rehabilitation process to iden- tify the feature 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.

1. Experimental evaluation
   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 capa- bilities. 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 encryp- tion, 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 rehabilita- tion 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

Homes (IHSH) in terms of network capacity and response time. Results obtained during the experimentations are given in [Table 2](#_bookmark27). More clear from the tabulated observation, the proposed SECHS model takes only less network capacity of 130 (kbps) while com- paring 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 initi- ating 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 adap- tive 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 pre- diction time and accuracy. According to obtained results given in [Table 3](#_bookmark28), the proposed adaptive weighted probabilistic classifier model outperforms the existing classifiers in both aspects. There- fore, the adaptive weighted probabilistic classifier obtains more robust performance due to the cloud-based deployment and effi- ciency 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]](#_bookmark55) and Boneh- Goh-Nissim homomorphic cryptosystem [[46]](#_bookmark57) schemes as given in [Table 4](#_bookmark28). 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 seman- tically 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 | 0.00107 | 96.9 |

Probabilistic

Table 4

Performance measure of security schemes.

index of disease D*i* with cost as O(*k*). In future, the research work disease prediction. Final prediction result is represented in the 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 dis- ease prediction due to sharing of computational workloads among the real-time fog routers and cloud nodes [[47]](#_bookmark59). As a result, an hier- archical disease prediction mechanism can be enforced through peer-to-peer communication and data offloading among the fog routers and cloud nodes.

1. Conclusion and future enhancement

Types of Security

Types of Defending Against Attacks

In this research, a layered architecture of secure edge-cloud-

Schemes

Plain Text Attack

Collusion Attack

External Eavesdropping Attack

Replaying Attack

based healthcare system is presented for real-time disease predic- tion with diagnosis and rehabilitation facility. The proposed sys- tem incorporates privacy preserving additive homomorphic

Privacy-preserving self helped medical diagnosis

Boneh-Goh-Nissim homomorphic cryptosystem

Proposed additive homomorphic encryption

No Yes Yes No

Yes No Yes No

Yes Yes Yes Yes

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 geo- graphic locations were processed in a cloud layer using the pro- posed 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 proba- bilistic model during the processing of patient data tasks. To vali- date the performance of proposed secure edge-cloud-based

both edge and cloud platforms without any collusion attack. In case of eavesdropping attack, all the schemes have defending capa- bility 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 com- munication 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 replay- ing 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 sys- tem not only verifies the cipher-text during data transmission but also verifies the freshly generated timestamp in each transmis- sion. In order to improve the diagnosis level, all the hospitals con- tinue 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 pro- posed 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 q* and random numbers H includes

O(*d*3) and O(*d*2) costs respectively. Next, the transmission cost of *n* number of encrypted data to the cloud node is O(*n* \* *d*2). Predic- tion system setting complexity is measured as O(*n* \* *d*3) dependent on *n* number of trait vectors Åp present in the medical database *D*^ .

p

*i*

ing of patients on cloud nodes is O(*m* \* *d*3), where *m* represents the Then, the time complexity of diagnosis and rehabilitation monitor- number of probabilistic prediction models employed during

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 pri- vacy preservation of patients’ electronic healthcare records.

Declaration of Competing Interest

The authors declare that they have no known competing finan- cial 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/](https://doi.org/10.1016/j.comcom.2020.02.018) [10.1016/j.comcom.2020.02.018](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/](https://doi.org/10.1016/j.future.2016.12.027) [j.future.2016.12.027](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/](https://doi.org/10.1016/j.future.2017.09.002) [10.1016/j.future.2017.09.002](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/](https://doi.org/10.1016/j.smhl.2018.04.001) [j.smhl.2018.04.001](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/](https://doi.org/10.1145/3230641) [3230641](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.](https://doi.org/10.1109/TNET.2019.2914189) [org/10.1109/TNET.2019.2914189](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/](https://doi.org/10.1016/j.future.2018.12.044) [j.future.2018.12.044](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/](https://doi.org/10.1016/j.compeleceng.2018.11.009) [j.compeleceng.2018.11.009](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-](https://doi.org/10.1007/s11276-019-02084-6) [019-02084-6](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/](https://doi.org/10.1016/j.future.2018.04.008) [10.1016/j.future.2018.04.008](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/](https://doi.org/10.1016/j.comcom.2018.08.004) [10.1016/j.comcom.2018.08.004](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.](https://doi.org/10.1016/j.jcss.2017.03.001) [jcss.2017.03.001](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>.

1. 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://](https://doi.org/10.1016/j.sysarc.2020.101776) [doi.org/10.1016/j.sysarc.2020.101776](https://doi.org/10.1016/j.sysarc.2020.101776).
2. 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/](https://doi.org/10.1016/j.future.2019.10.010) [10.1016/j.future.2019.10.010](https://doi.org/10.1016/j.future.2019.10.010).
3. 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/](https://doi.org/10.1016/j.comnet.2018.01.038) [j.comnet.2018.01.038](https://doi.org/10.1016/j.comnet.2018.01.038).
4. 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>.
5. 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](https://doi.org/10.1007/s11277-020-07251-z).
6. 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/](https://doi.org/10.1016/j.ijmedinf.2016.03.001) [10.1016/j.ijmedinf.2016.03.001](https://doi.org/10.1016/j.ijmedinf.2016.03.001).
7. 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>.
8. 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>.
9. 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.](https://doi.org/10.1016/j.eswa.2018.08.021) [eswa.2018.08.021](https://doi.org/10.1016/j.eswa.2018.08.021).
10. 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/](https://doi.org/10.1016/j.future.2015.11.010) [j.future.2015.11.010](https://doi.org/10.1016/j.future.2015.11.010).
11. 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>.
12. 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.](https://doi.org/10.12720/jcm.12.4.228-233) [org/10.12720/jcm.12.4.228-233](https://doi.org/10.12720/jcm.12.4.228-233).
13. 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.
14. 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.
15. 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-](https://doi.org/10.1186/1475-925X-6-23) [925X-6-23](https://doi.org/10.1186/1475-925X-6-23).
16. 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.
17. 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>.
18. 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>.
19. 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>.