Cluster Computing (2023) 26:1205–1220
https://doi.org/10.1007/s10586-022-03717-w

Edge computing based secure health monitoring framework for electronic healthcare system

Ashish Singh[1] · Kakali Chatterjee[2]

Received: 24 January 2022 / Revised: 7 July 2022 / Accepted: 3 August 2022 / Published online: 2 September 2022

Abstract
Nowadays, Smart Healthcare Systems (SHS) are frequently used by people for personal healthcare observations using various smart devices. The SHS uses IoT technology and cloud infrastructure for data capturing, transmitting it through smart devices, data storage, processing, and healthcare advice. Processing such a huge amount of data from numerous IoT devices in a short time is quite challenging. Thus, technological frameworks such as edge computing or fog computing can be used as a middle layer between cloud and user in SHS. It reduces the response time for data processing at the lower level (edge level). But, Edge of Things (EoT) also suffers from security and privacy issues. A robust healthcare monitoring framework with secure data storage and access is needed. It will provide a quick response in case of the production of abnormal data and store/access the sensitive data securely. This paper proposed a Secure Framework based on the Edge of Things (SEoT) for Smart healthcare systems. This framework is mainly designed for real-time health monitoring, maintaining the security and confidentiality of the healthcare data in a controlled manner. This paper included clustering approaches for analyzing bio-signal data for abnormality detection and Attribute-Based Encryption (ABE) for bio-signal data security and secure access. The experimental results of the proposed framework show improved performance with maintaining the accuracy of up to 98.5% and data security.

Keywords Electronic healthcare system · Edge computing · SEoT · Attribute-based encryption · Secure health monitoring · Clustering · Data security and privacy

1 Introduction

Health is a basic need of a living being. A good healthcare system of a country is a vital parameter to reflect its developmental growth. India has a vast population, ranked 2nd in the world. The huge population and diversity in the living conditions of individuals in the country make it quite challenging to provide a good, uniform health care service. With the digital revolution in the healthcare sector, SHS came into existence. SHS facilities to the people with the help of various technologies and smart devices. The technological development phases in SHS have travelled from 1.0 to 4.0 technology version of the healthcare framework [1]. The key focus of these frameworks was from doctor-centric to Electronic Health Record (EHR), to patient-centric, to cloud technologies, respectively. The IoT-based SHS framework is a network of interconnected smart devices that sense, analyze and provide remote healthcare solutions to people. Various wearable or implementable medical devices with embedded healthcare sensors are continuously used to capture a person's basic health parameters. Through the observation and analysis of the gathered data, customized healthcare suggestions are provided to the particular person. So, this IoT-based SHS model is a good solution for providing better healthcare services. A major disadvantage of this model is that the storage and security of the huge amount of continuously gathered data are challenging tasks for the traditional storage system. Thus, various healthcare providing

✉ Kakali Chatterjee
kakali@nitp.ac.in

Ashish Singh
ashishashish307@gmail.com

[1] School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha 751024, India

[2] Department of Computer Science and Engineering, National Institute of Technology, Patna, Bihar 800005, India

agencies' cloud-enabled data processing and storage solutions emerged called Cloud of Things (CoT). The key requirement of a good SHS is its quick responsiveness and data security. It has been observed that the cloud-based SHS model suffers from various challenges in catering for these requirements. It suffers from high service latency due to long-distance transmission between the user and the cloud centre. The low network bandwidth and transmission speed reduce the system's efficiency while processing massive data and multiple queries. Various security measures have been applied to counter real-time data security threats. It also reduces system responsiveness in emergency cases. So, considering all these issues, EoT-based SHS provides a promising solution. Edge Computing (EC) is an essential part of smart healthcare to make autonomous judgments and real-time healthcare monitoring [2]. It uses a decentralized architecture with data processing at the edge of the frontier network nodes [3]. Before connecting to the cloud, the EC layer will complete activities locally, lowering network overhead. EC can also be easily integrated with other wireless networks [4–7] to solve network and computational issues. The benefits of Smart Healthcare systems (SHS) are low-cost treatment, high-quality care, effective data management and sharing schemes, online accessibility, rapid elasticity, and many more [8, 9]. Data processing near the data sources also improves the Quality of Service (QoS) for delay-sensitive services. For example, EC-enabled ambulance services are equipped with predictive algorithms to make judgments without human intervention in healthcare. Furthermore, EC faces many challenges in network setups, wireless network integration, the accuracy of quick decisions, data privacy, and many more. The technological growth and smart functionality of edge-based SHS bring several threats and attacks.

This research work mainly focuses on two research problems of EC-based SHS. The first research problem is the efficient analysis of the data acquired in the edge server during remote health monitoring, which will make the final decision for the patient treatment. For example, Critical congenital heart disease (CCHD) patients suffer heart defects from birth and need constant monitoring. However, the COVID 19 pandemic makes it impossible to visit the hospital regularly. In such cases, constant measurement with an accuracy of Blood pressure, heart rate and rhythm, and respiratory rate is essential. Another issue is that this sensitive healthcare data is kept in the public cloud as Patient Health Information (PHI). Smart community users can easily access this PHI. The open public cloud for storing sensitive PHI brings new security threats and data access issues. Many data security approaches [10–14] have been proposed in this direction. The author of [10] has proposed a homomorphic encryption data security model. It can perform data analysis in encrypted mode, reducing the chances of intruders' misuse. However, using this encryption method will make data search operations difficult. Whenever the healthcare givers want to search the desired patients' EHR, the whole data must be decrypted and again encrypted. So, this process will create a huge bandwidth overhead for the model. Hence, the main motivation of this paper is to build a SEoT framework based on edge computing to deal with these present two issues for time-critical healthcare applications.

The first research problem can be overcome by using a clustering approach that can be used for the decision-making of the monitored data. In a smart monitoring system, sensors capture bio-signal data of critical care patients. This data is aggregated and analyzed for decision-making remotely by the medical personnel. The clustering-based approach measures the similarity between sample data using the distance vector method. It can act as an efficient analytic tool to determine the abnormality in a given user's continuously observed health parameter by putting it into different clusters. For example, clustering different types of observed pulse rates and SPO2 levels of a person can indicate the severity of a chest infection. ABE-based access mechanism can preserve this sensitive data's privacy while stored on the medical server. This encryption strategy can help maintain data confidentiality while sharing it with stakeholders.

Hence, the contributions of the paper are

- This paper proposed the SEoT framework for secure remote health monitoring and emergency services.
- It uses a clustering approach for data gathering and aggregation. It will help medical personnel with quick decision-making.
- An ABE technique with an access policy has been included in the SEoT framework to maintain high-level security and access control with low cost and latency.
- The performance and outcome of the proposed framework securely show better abnormal data detection.

The remaining sections of this paper are organized as follows: Sect. 2 discusses the related works. Section 3 describes the proposed SEoT framework. Section 4 discusses the experimental evaluation of the proposed SEoT framework. The implementation and result of the proposed framework are analyzed in Sect. 5. The conclusion of this research work is presented in Sect. 6.

2 Related work

Technological advancement such as IoT, CoT, and EoT in the healthcare sector has completely revolutionized the human world. Various issues and challenges have been observed in the transition from the 1.0 to 4.0 technology version of the healthcare framework [15]. A few major

challenges are data security, storage, service latency, network bandwidth etc. Various research works [16–21] has been done to tackle these issues in SHS. In [22] IoT-based healthcare framework is proposed to process multimedia data. The use of blockchain technology makes it secure, transparent and controlled access to patient records and shipment processes. Authors claim success rate over the ratio of product drop, attacks line falsification, and wormhole based on simulation result is 86% better than existing works using blockchain technique. The Trust of nodes is calculated after a specific interval, improving performance. In [14] Ciphertext-Policy ABE (CPABE) technique has been used to encrypt healthcare data. In [23] an IoT-based healthcare system has been proposed using particle swarm optimization. It provides an early warning system by detecting the physical conditions in advance for getting treatment accordingly. An IoT and the cloud-based healthcare system in the home environment for assisted living have been proposed in [24]. The model consists of an intelligent medicine box including iMedBox, iMedPack, and Bio-Patch. These boxes provide services like real-time monitoring of bio-signals, data analysis, raising the alarm, remote prescription, remote diagnosis, and medication. In [25], an IoT and cloud-based monitoring system with machine learning has been proposed. It includes GPS tracking modules to provide real-time healthcare support to the soldiers. It uses different sensors, including bomb detector sensors, which enhance the security of soldiers' lives. In [10], the author proposed a smart health surveillance framework using Fully Homomorphic Encryption (FHE) and a machine learning-based clustering technique. In [26] an IoT-based healthcare system is proposed, where patient data is protected using attribute-based encryption with cross-domain support. The patient's encrypted medical data is accessible by authorized users in normal situations. The break-glass access mechanism enables accessing files of the patient's medical history in emergencies. The deduplication technique removes redundant data and reduces transfer overhead. IoT-based healthcare framework is proposed in [22]. It can process multimedia data. The use of blockchain technology makes it secure, transparent and controlled access to patient records and shipment processes. Authors claim success rate over the ratio of product drop, attacks line falsification, and wormhole based on simulation result is 86 using blockchain technique. The Trust of nodes is calculated after a specific interval which improves the performance. The author in [27] proposed a framework that is scalable semantically based on IoT, detecting epidemics early. It uses an engine called Complex Event Processing (CEP) to detect abnormal events in Daily Living Activity (ADL). He processes data if it finds any deviations in ADL. An updated version of semantic message-oriented middleware architecture (SeMoM) reduces complexity and scalability.

The HealthFog framework based on Edge Computing devices with deep learning has been proposed in [28]. It can automatically analyze heart disease to provide lightweight fog or healthcare services and efficiently manage heart patients' data from IoT devices. In [29], blockchain and ABE techniques have been used to protect medical data. The CPABE technique has been used in [30] to maintain the secure monitoring of healthcare data. In [31], IoT, cloud and edge-based healthcare systems with blockchain have been proposed to provide data security during monitoring. Homomorphic encryption based on mutual privacy-preserving using the K-means strategy ensures the protection between participants and the cluster centre [32]. The authors in [33] have proposed an IoT with a cloud-based healthcare system. It uses an IP-based multimedia service called IP Multimedia Subsystem (IMS) to monitor patients' health conditions remotely. The Session Initiation Protocol (SIP) communicates with the IMS core and transmits data. This system can handle emergencies by implementing an alert system which makes calls and sends messages automatically in real-time. The sources of data are sensors, apps, and smartwatches. In [34], the authors have developed a static scheduler for Voltage and Frequency Scaling (DVFS) integrated IoT-based healthcare applications for streaming in real-time. It is energy efficient and uses Network-on-Chip (NoC), Multiprocessor System-on-Chips (MPSoCs), and Voltage Frequency Island (VFI). The scheduler is based on nonlinear programming. The Re-Timed conditional task graph is a pipelining software approach of task-level coarse-grained reduces re-timing latency with constant energy consumption. In [35] Privacy-Preserving Searchable Encryption technique has been used in which decryption is not required for searching data in the cloud. In [36], CP weighted ABE has been used to ensure data security with weighted attributes on the Internet of Health Things. The author in [37] has proposed an EoT-based scalable and efficient healthcare solution. In [38], a blockchain-based data protection scheme has been proposed. The paper [39] proposes an access control scheme for a cloud-based E-Healthcare system. From the above literature works, the following research problems are identified:

- The lack of uniformity among connected devices reduces the accuracy of the data.
- Massive data being transferred and stored can be hacked and misused.
- The cost in terms of communicational and computational cost is very high for constrained devices.
- High latency and response time degrade the Quality of Services (QoS) parameter in the cloud-based healthcare system.

3 Proposed framework

This section discusses the proposed SEoT framework for remote health monitoring and emergency services. The proposed framework consists of mainly four layers: the Data generation layer, Edge computing layer, Cloud storage layer, and the smart healthcare community, as shown in Fig. 1. The sensors in different devices collect the healthcare data of a person in the data generation layer. The data is then transferred to the edge layer through the gateway devices. In the edge computing layer, the edge server is responsible for keeping all details of secure patient data stored in the cloud. It also operates clustering techniques to determine the abnormal patient data. All collected data from the body sensors are transferred to the edge layer and then from the edge layer to the medical server in the cloud storage layer. This edge layer includes an encryption module with an access policy, ensuring patient data integrity and confidentiality. During data retrieval, first, the authentication is performed. After that, search tokens have been generated, which helps to find the data pointer. The Patient ID (PID) data pointer is sent to cloud storage to retrieve patient data.

In the proposed framework, the novelty is applied in two phases: one phase consists of a *Data abnormality Detection* using the clustering-based approach, which is applied at the edge level. Another includes *Data Security using Attribute-Based Encryption (ABE)* technique with access policy. It helps in detecting abnormal data. It helps to perverse the privacy of sensitive data without adding much overhead to the system.

3.1 Data abnormality detection

The proposed framework collects continuous bio-signals of the user of the system. Observing the usual/normal bio-signal value variation may indicate user health abnormality. So, by applying the clustering approach to the observed data, it will be easy to figure out the deviation in the observed bio-signal value. Thus, the first phase's aim includes making a cluster for different data values. It enables the system to analyze and detect abnormal changes in bio-signal data. The different clustering-based approaches were used to make the cluster. These approaches are K-means clustering (KMC) [10], First Nearest Neighbors (FNN) [40], All Nearest Neighbors (ANN) [40], and K-Medoid based Nearest Neighbors (KMNN) [40].

- *KMC* It is an unsupervised learning algorithm used to solve the clustering problem in data science. This approach aims to partition n observations into k clusters

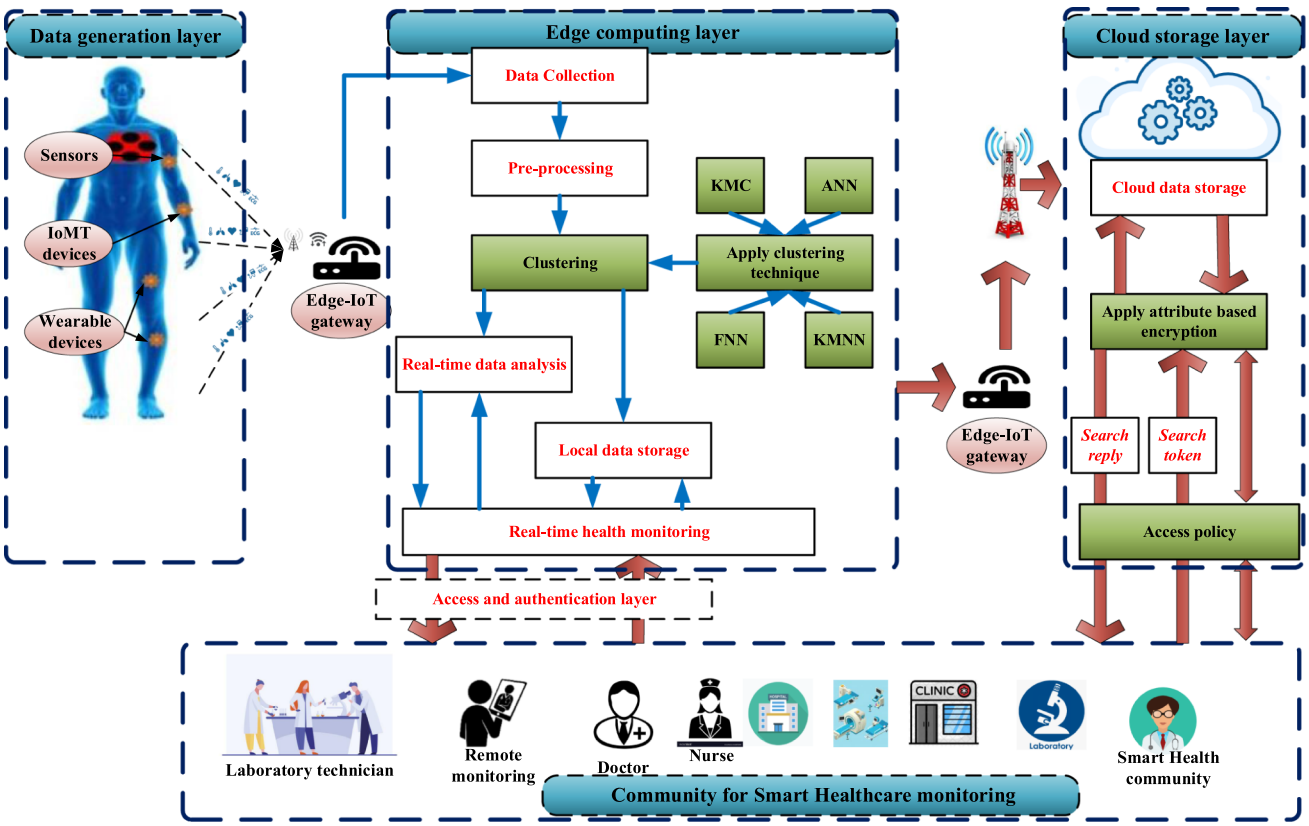

Fig. 1 Proposed edge computing based secure health monitoring framework

in which each observation belongs to the cluster with the nearest mean. The algorithm takes the unlabeled dataset as input. It divides the dataset into different clusters based on the closest k-centre. For every data point, find the closest centroid using the distance measurement Euclidean Distance. Now, assign the data point to the closest centroid. The founded centroid is the average of all data points assigned to it. Algorithm 1 presents the pseudocode of KMC.

- *FNN* This algorithm mainly solves the travelling salesman problem. The dataset's first data object is the most similar to the input data. Suppose the next data object is to be found more similar to the new data object. In that case, it can be labelled as most similar and replace the old data object.
- *ANN* It is a proximity searching technique which is used to solve the optimization problem. It computes the nearest neighbour for each of the input points. The pseudocode of this algorithm is presented in Algorithm 1. In this algorithm, all similar neighbour data object information is stored. All these data object information are included in determining the conclusion at each stage.
- *KMNN* This algorithm is an extension of KMC with more robust noise cancellation. The low complexity of the algorithm makes it more suitable for smaller datasets. It is the combination of KMC and K-Medoid in which the closest nearest neighbour is used for computation purposes. It tries to reduce the sum of distances between each data point and the Medoid of its cluster. Medoid is the central cluster point with a minimum distance to other data points.

3.2 Data security using ABE with access policy

Our proposed model applies the ABE encryption technique before storage to perverse the privacy of sensitive data in the cloud layer. This technique uses a Cipher Policy Attribute-Based Encryption (CPAB) with hierarchical property to support the scalability by delegating the key generation task to next-level authority. Here, the hospital management is the trusted party known as Root Master (RM). Multiple domains, such as diagnosis, treatment, pharmacy, insurance etc., can be domain masters (DM). This phase will execute three algorithms. They are - ATREE_GEN( ) , MKEY_GEN ( ), TOK_GEN ( ) algorithm.

Algorithm 1 Clustering algorithms: KMC, FNN, ANN, and KMNN

```
procedure INPUT:(Testing Data objects (D) )
    OUTPUT: Clusters (C)
KMC:
    Choose a random K for number of cluster in a given data objects.
    for all the data objects do
        Select random K points or centroid.
        Euclidean distance is used to measure the distance between each data object and cluster centroids.
        The minimum Euclidean distance is used to assign each data object to a cluster centroid.
    end for
    Prepare the cluster based on the assign data objects.
FNN:
    for all the data objects do
        SimD ← The first most similar data object from D.
        C ← Assign the data object as SimD
    end for
ANN:
    for all the data objects do
        Sim_neigh_info ← All similar neighbour data object information from D.
        C ← Assign most repeated data objects in Sim_neigh_info.
    end for
KMNN:
    for all the data objects do
        Sim_neigh_info ← All similar neighbour data object information from D.
        C ← Compute clustering on Sim_neigh_info and find two clustering heads.
        s ← compute: ∑ distance (Sim_neigh_info - clustering heads)
        S ← Stored s.
        S' ← 20% of the last data objects are removed.
        C ← Assign data objects which are in S'.
    end for
end procedure
```

Table 1 Index table (T_1) for attribute generation

Domain	Attribute	Attribute ID	Label	Codeword
D_1	Diagnosis	LID 01 RID 01	1	011 (C_3) 010 (C_4)
D_2	Treatment	LID 00 RID 00	1	001 (C_6) 000 (C_5)
D_3	Symptoms	LID 011 RID 011	2	0100 (C_{10}) 0101 (C_9)
D_4	Test report	LID 010 RID 010	2	0110 (C_8) 0111 (C_7)
D_5	Therapy	LID 000 RID 000	2	0000 (C_{14}) 0001 (C_{13})
D_6	Surgery	LID 001 RID 001	2	0010 (C_{12}) 0011 (C_{11})

3.2.1 ATREE_GEN( )

Each domain will generate the secret key for the next level. So, the hospital management will generate the secret key for each domain (diagnosis/treatment). The RM's role is to manage different domains and distribute system parameters. The Domain Manager (DM) is responsible for managing attributes by creating subdomains (D). Different domain managers manage domains like medical history, illness, insurance, etc. We assign a set of attributes in each domain in the tree-like structure. An index table (T_1) for attribute generation is presented in Table 1. Now, the construction of the tree matrix is given below-

Step 1 The DM is assigned with a value of '1' in the left node, and the right is assigned '0'. Suppose the left node (LID) has a sub-domain name Diagnosis (D_1) and the right node (RID) have a sub-domain name Treatment (D_2). The sub-domain D_1 and D_2 are represented with codeword $C_1 = 01$ and $C_2 = 00$. This label is defined as label 1 with the secret key. In this way, each attribute is presented in a tree structure.

Step 2 Each attribute will assign a unique value using a codeword to identify it easily. The attribute tree of order (depth) n = n_i has 2^n terminal nodes. The label 2 attributes are primary attributes of the sub-domain D_1. For example, attribute such as Symptoms and Test Reports is represented as codewords C_3 and C_4 where $C_3 = 011$ and $C_4 = 010$. Similarly, under level 2, another sub-domain D_2, which is termed as "Treatment"having Primary attributes "Medicine"and "Therapy"represented as codewords C_5 and C_6 with codeword $C_5 = 001$ and $C_6 = 000$.

Table 2 Index table (T_2) for master key generation

Domain	Label	Codeword	Key location	Generated key
D_1	1	$C_1(01)$	3	21
D_2	1	$C_2(00)$	4	22
D_1	2	$C_3(011)$	5	31
D_1	2	$C_4(010)$	6	32
D_2	2	$C_5(001)$	7	41
D_2	2	$C_6(000)$	8	42
D_4	3	$C_7(0111)$	9	51
D_4	3	$C_8(0110)$	10	52
D_3	3	$C_9(0101)$	11	61
D_3	3	$C_{10}(0100)$	12	62

Step 3 Now, each primary attribute has some secondary attributes represented in the next label, i.e. Label 3. In this label, all attributes related to each primary attribute are placed. So under D_1, the node (D_4) will represent attributes as codewords C_7 and C_8 with codeword $C_7 = 0111$ and $C_8 = 0110$. Similarly under D_2, the node (D_3) will represent attributes as codewords C_9 and C_{10} with codeword $C_9 = 0101$ and $C_{10} = 0100$. In this way, the attributes are represented in a tree structure. The algorithm constructs a tree representing the attributes as a codeword. It generates a master key for each level using the MKEY_GEN algorithm.

3.2.2 MKEY_GEN ( )

Step 1 In this key generation process, MKEY_GEN() algorithm will execute. The algorithm is explained with an example. In this algorithm, we first store the innovation bits '0'and '1'in location 1 and location 2, respectively. Now, in label 1, two codewords $C_1 = 01$ and $C_2 = 00$ have generated the secret key $K_1 = 21$ and $K_2 = 22$ with their locations i.e. location 3 and location 4.

Table 3 Search key generation table (T_3)

Keyword (attribute name)	DOC_id	Encrypted index	Search token
ATTR_NM(W_1)	DID_1	$ENC[W_1 \| \| DID_1]$	$C_1 \| \| DP_1$
ATTR_NM(W_2)	DID_2	$ENC[W_2 \| \| DID_2]$	$C_2 \| \| DP_2$
ATTR_NM(W_3)	DID_3	$ENC[W_3 \| \| DID_3]$	$C_3 \| \| DP_3$
ATTR_NM(W_4)	DID_4	$ENC[W_4 \| \| DID_4]$	$C_4 \| \| DP_4$

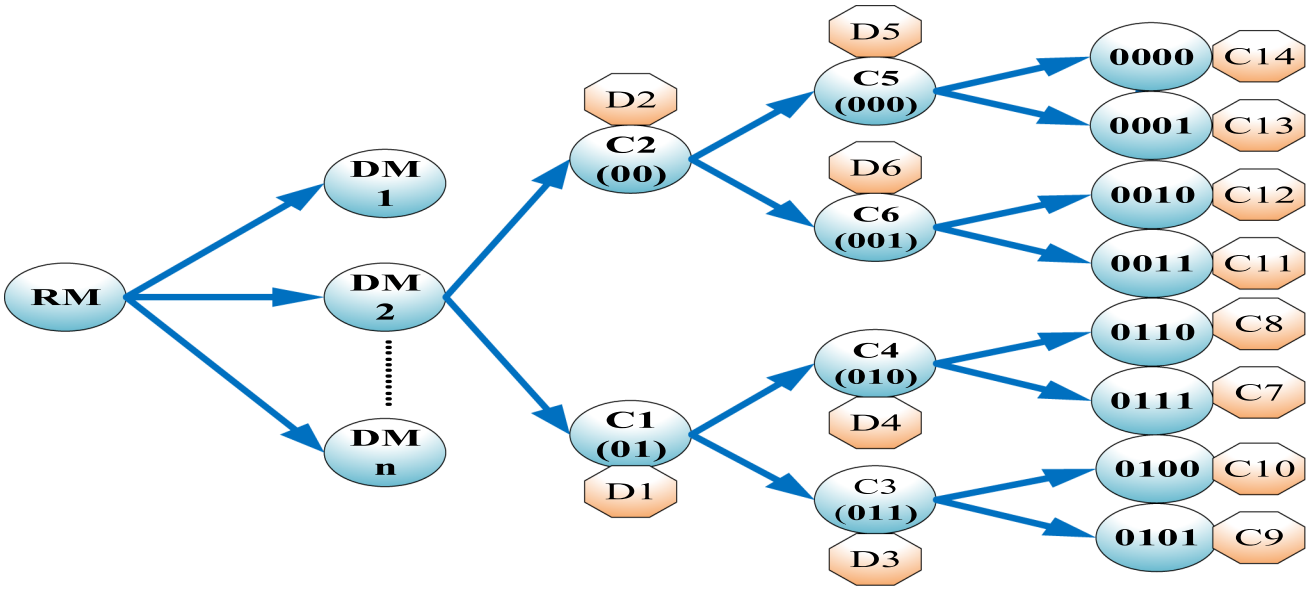

Fig. 2 Attribute tree

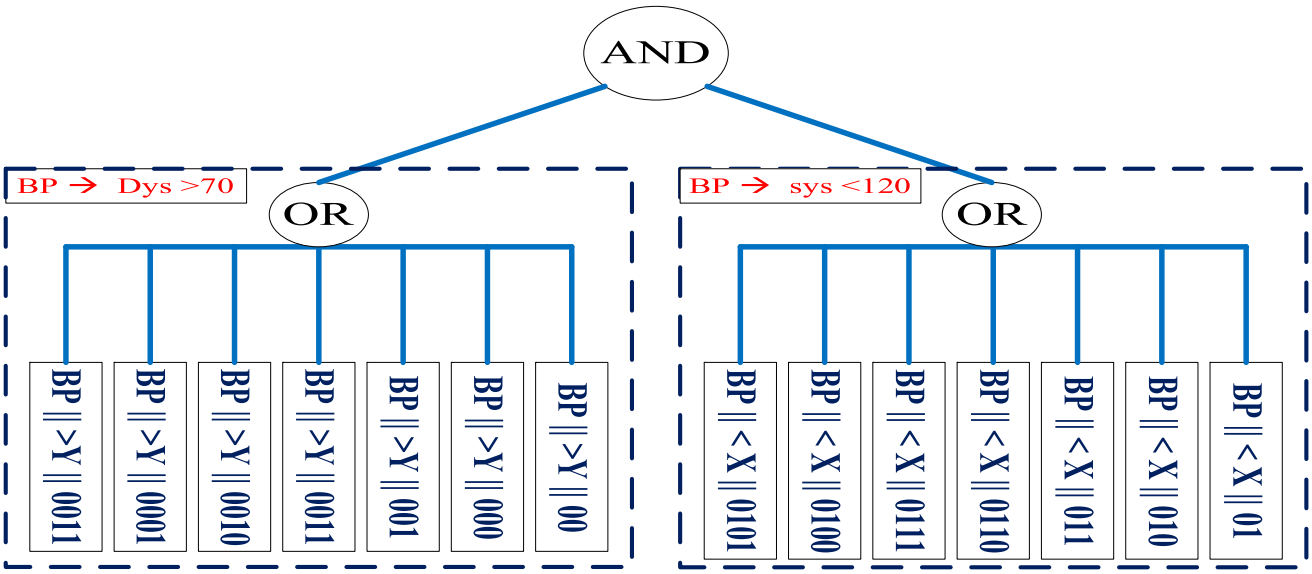

Fig. 3 Policy tree for proposed model

Step 2 In this step, the next lebel i.e lebel 2 key generation is performed with the two codewords $C_3 = 011$ and $C_4 = 010$ have generated the secret key $K_3 = 31$ and $K_4 = 32$ with their locations i.e. location 5 and location 6. Then the other two codewords $C_5 = 001$ and $C_6 = 000$ have

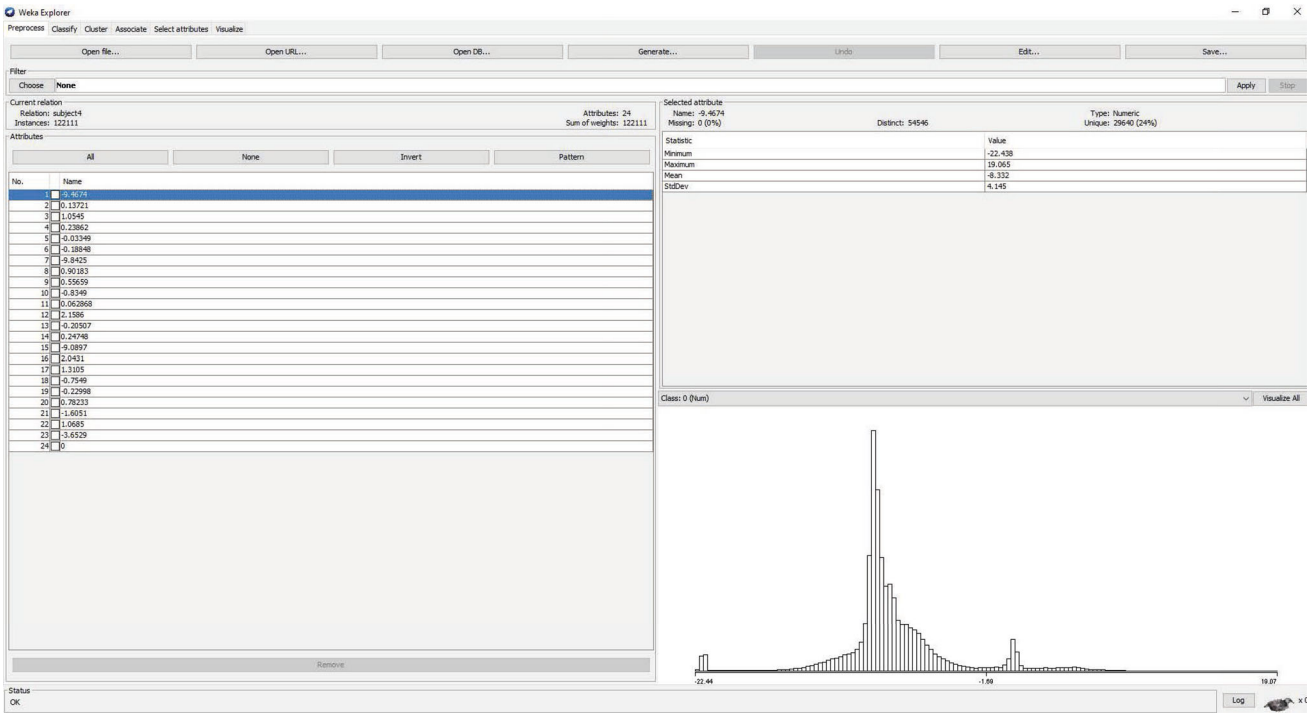

Fig. 4 Statistic values while selecting the first attribute of subject 4

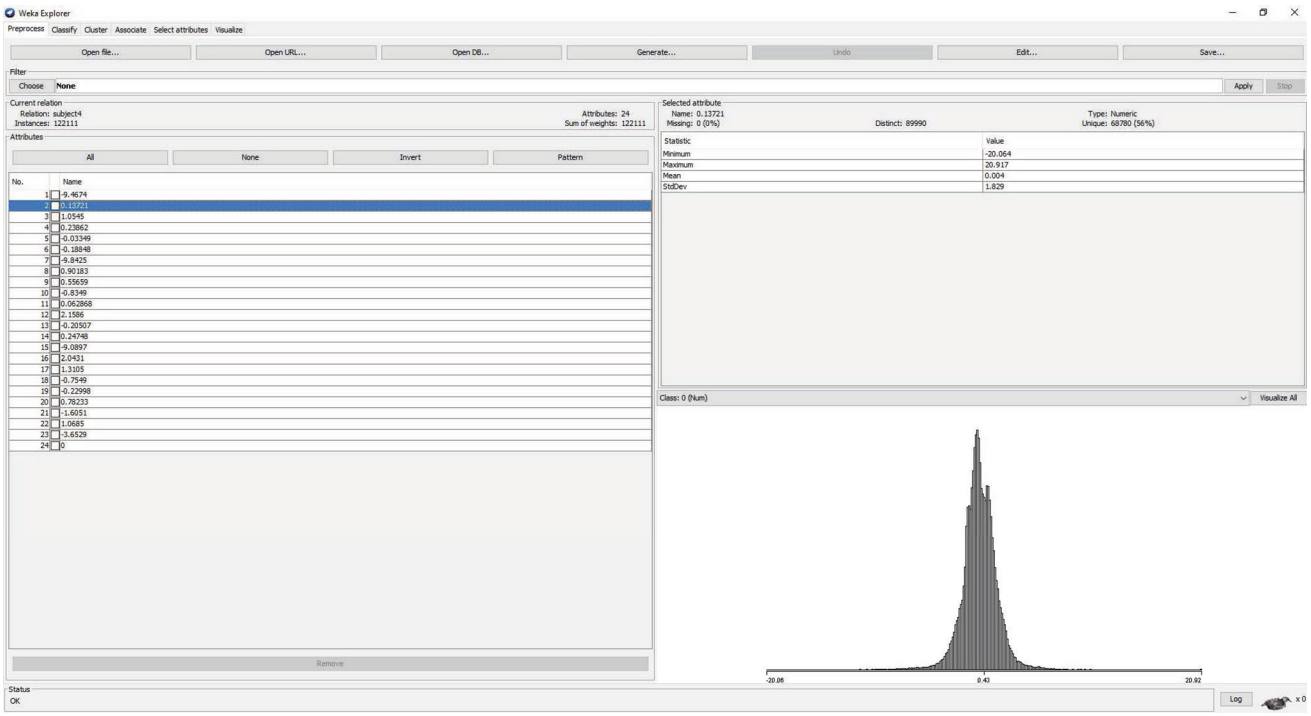

Fig. 5 Statistic values while selecting the second attribute of subject 4

generated the secret key $K_5 = 41$ and $K_6 = 42$ with their locations i.e. location 7 and location 8.

Step 3 In this step, the next lebel i.e lebel 3 key generation is performed with the two codewords $C_7 = 0111$ and $C_8 = 0110$ have generated the secret key $K_7 = 51$ and $K_8 = 52$ with their locations i.e. location 9 and location 10. Then the other two codewords $C_9 = 0101$ and $C_{10} = 0100$ have generated the secret key $K_9 = 61$ and $K_{10} = 62$ with

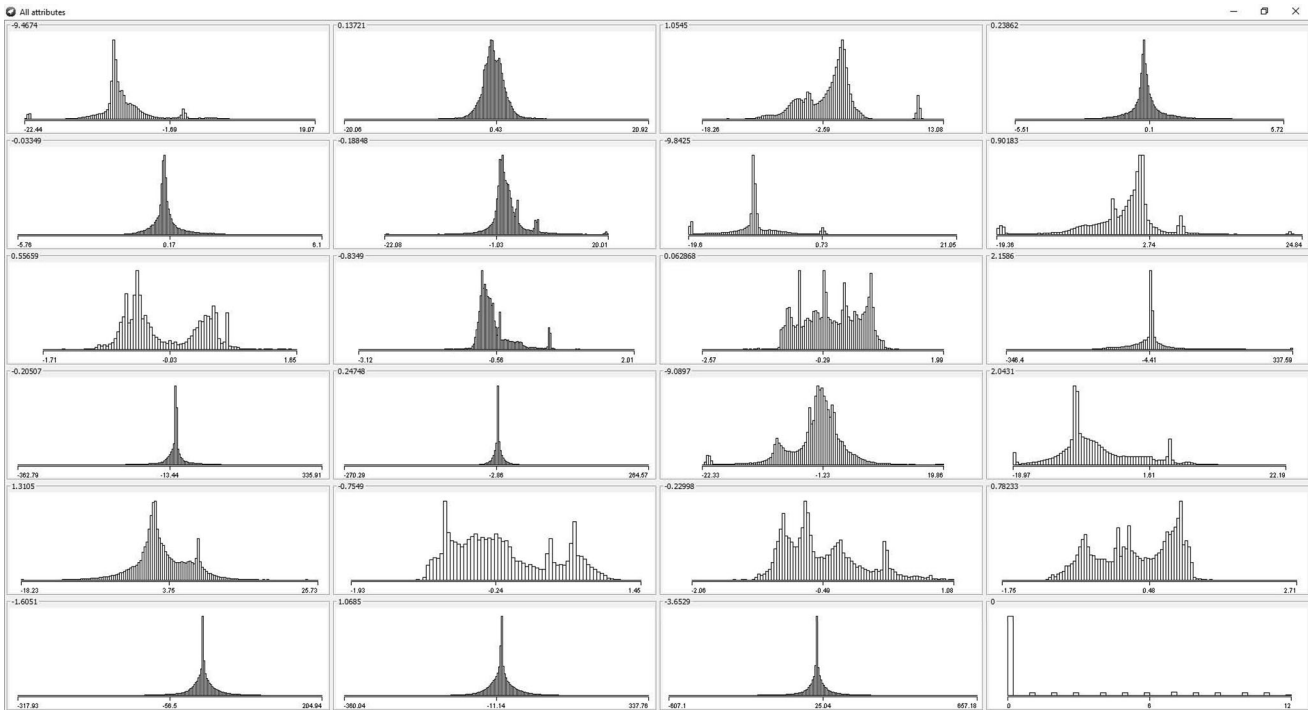

Fig. 6 Statistic values of all attributes of subject 4

their locations i.e. location 11 and location 12. In this way, the key structure will be generated. The described algorithmic parameters are listed in Index table (T_2) Table 2.

3.2.3 TOK_GEN ( )

Step 1 A Search Token (ST) will be generated by including user input as a search keyword (which is defined by Attribute Name (AT). The search token for a keyword (attribute name) is computed with all combinations of codewords. The token is generated with the codeword and Data Pointer (DP). Here, we use key location as DP.

Step 2 ST is used to find the document ID (DID) from the index table of codeword and data pointer. With the help of mapping Table 2, the key location can be traced.

Step 3 Data pointer used to find the secret key of the corresponding attribute IDs which match the search token and send back the corresponding document to the user with that attribute.

Step 4 The decryption can be carried by DECKdoc (D_i), including a secret key. The parameter details of search key generation are summarized in table (T_3) Table 3.

3.3 Access policy

The data owner creates the access policy for each attribute of EHR. In the scheme, the access policy is based on the access structure of the EHR. In the access structure, each intermediate node represents a threshold gate and each leaf node represents the attribute of the data user. If a node has a total N number of child nodes and T is the threshold value for all user attributes, then for T == 1 corresponding node is OR-Gate and for T == N, the node is AND-Gate. In this access policy, each domain, such as "diagnosis", "treatment", etc., is designed in an attribute tree shown in Fig. 2. The access policy is defined so that each value contains a 1 or 0-bit string for comparable attributes such as "Blood Pressure (BP)"in the "diagnosis"domain. For example, the access policy of "BP", which is one of the attributes in "Diagnosis,"is "(Systolic (X) $<$ 120 AND Diastolic $>$ 70)". These values are converted into a binary string, and the policy structure is shown in Fig. 3.

4 Experimental evaluation

This section discussed the experimental evaluation and analyzed the results of the proposed SEoT model.

4.1 Experimental setup

An android executable-based platform has been developed for real-time health monitoring of healthcare data and emergency services securely. The IoT devices and sensors based on wired connection contain Arduino UNO R3

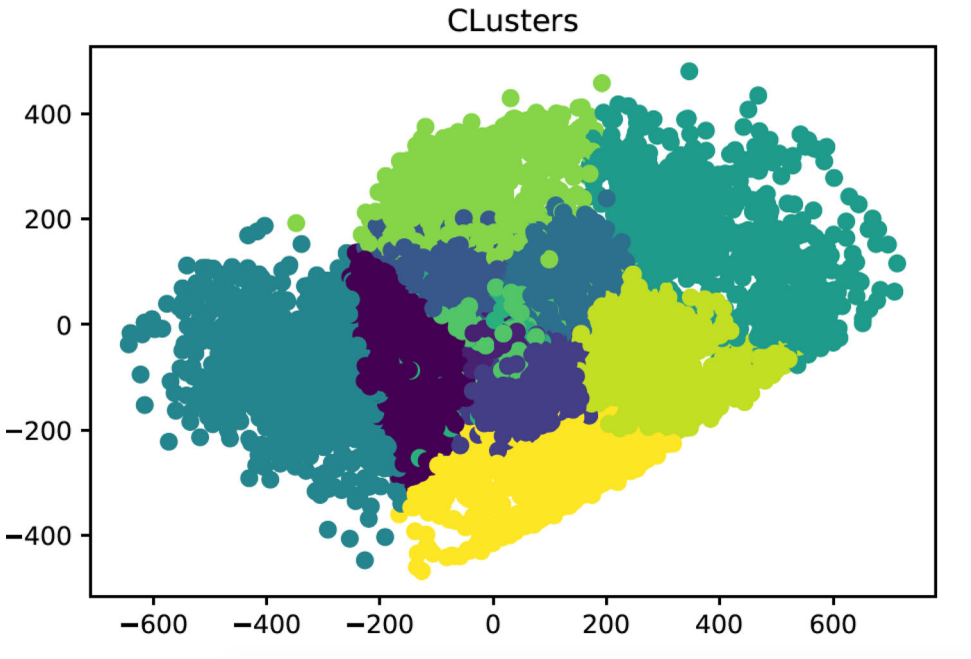

Fig. 7 Clustering result of subject 4

Board ATmega328P ATmega16U2 IoT device, multiple sensors (LM35, DHT11, MQ-9, MQ-35, ECG sensor, heartbeat sensor, SPD015GDN) for collection of patient body information. The used IoT device is a low-cost, lightweight, and breadboard-friendly board with a small physical size that supports various families of Linux. The secured framework is developed using Python high-level Multi-paradigm programming language and implemented on open-source Arduino Software (IDE) V-1.8.16.

4.2 Dataset description

For the experimental purpose, MHEALTH Dataset has been downloaded from the UCI Machine Learning Repository [41, 42]. The dataset contains 120 instances, 23 attributes, and 121781 web hits. This dataset is based on multimodal body sensing, which comprises body motion and vital signs of 10 volunteers performing several physical activities. The dataset includes 12 activities collected from three sensor devices, measuring 24 body sensing features. Shimmer3 wearable sensors have been implanted on the subject's chest, right wrist and left ankle to measure vital body parameters. 2-lead ECG measurements can be possible using the chest's implanted sensor, which monitors the basic heart conditions and arrhythmias. The data collected for each volunteer(subject) is stored in a different log file. Each log file contains the different sample values (by rows) recorded for all 24 body features (attributes) sensed by the three sensors placed on the human body (by columns).

4.3 Clustering approach

The clustering algorithms are used to measure the abnormal changes in MHEALTH Dataset [41, 42]. The first step is to import the MHEALTH Dataset into the Weka explorer (Weka Machine Learning tool). A snapshot of the Weka tool (after data import) is shown in Figs. 4 and 5. These two figures show only the data detail of one log file of the MHEALTH dataset (volunteer/subject 4) under different attributes for ease of understanding purpose. These results also illustrate the statistic values in terms of minimum, maximum, mean, and standard deviation. The statistic values are changed when the subject attribute value has been changed. Figure 6 shows the statistic values of all 24 attributes of subject 4, and Fig. 7 shows the clustering result after applying clustering algorithms to subject 4. The different cluster has been prepared to determine the accuracy of data value distribution among the cluster. Figure 8 shows the accuracy of four different clusters under different clustering algorithms. The graphical presentation of the result shows that KMNN clustering algorithm accuracy is better than the other three algorithms.

5 Performance and result analysis

After the experimental setup and data clustering, the performance of the proposed SEoT framework is calculated. All four abnormal data detection strategies using four different clustering approaches mentioned in the proposed algorithm 1 were used to measure the framework's

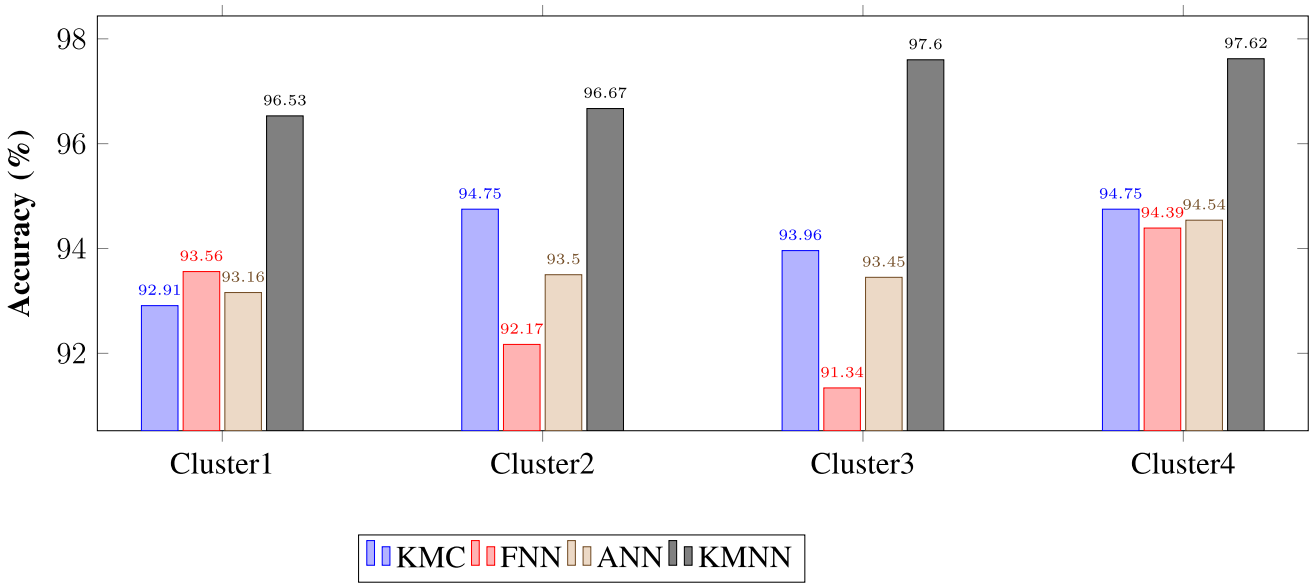

Fig. 8 Clustering accuracy of the proposed SEoT health monitoring framework

performance. In this work, the experiment has been performed on different dataset lengths to observe the scalability of the proposed framework. Three experiments were conducted with the dataset length of 50%, 75%, and 100% of the total dataset. The experimental data are again splitted into three parts with a ratio of 60:20:20. 60% of the dataset is considered a training sample, 20% is considered a validation sample, and the last 20% is considered a testing sample. All four clustering strategies (KMC, FNN, ANN, and KMNN) are considered during the implementation. Different data points (1000, 3000, 5000, and 8000) are also considered to determine the variation in results with respect to data points. The obtained results in terms of training, validation, and testing of different detection strategies are summarized in Table 4.

The proposed SEoT health monitoring framework is evaluated with the help of a confusion matrix containing several test metrics. These test metrics are precision, recall, f1-Score, Accuracy, False Positive Rate (FPR), and Area Under Curve (AUC). There are mainly four factors involved in the computation of these values. A detailed

Table 4 Training, validation, and testing accuracy (%) results of different detection strategies

Dataset length	Algorithm	Data points											
		1000			3000			5000			8000		
		Train	Valid	Test	Train	Valid	Test	Train	Valid	Test	Train	Valid	Test
50%	*KMC*	98.35	98.28	98.37	98.17	98.16	98.08	99.67	99.68	99.69	98.59	98.58	98.43
	FNN	98.33	98.38	98.48	98.25	98.26	98.27	98.57	98.47	98.66	98.44	98.38	98.59
	ANN	98.23	98.35	98.46	97.16	97.18	97.19	97.11	97.12	97.13	98.46	98.29	98.36
	KMNN	98.16	98.25	98.16	97.88	97.82	97.82	97.31	97.33	97.34	98.51	98.33	98.33
75%	*KMC*	95.81	95.62	95.73	97.84	95.58	97.67	97.84	97.85	97.86	98.55	98.84	98.78
	FNN	97.02	97.01	97.12	97.18	98.02	98.01	97.04	97.03	97.04	98.73	98.66	97.52
	ANN	97.62	97.41	97.35	97.12	97.13	97.13	97.88	97.89	97.90	98.44	98.42	98.40
	KMNN	96.88	96.45	96.89	97.85	97.86	97.87	97.91	97.92	97.93	98.52	98.50	98.48
100%	*KMC*	91.31	91.11	91.19	98.82	98.80	98.81	97.11	97.15	97.17	98.43	98.42	98.44
	FNN	98.71	98.67	98.88	98.22	98.23	98.24	97.16	97.18	97.20	98.31	98.16	98.18
	ANN	98.29	91.11	91.79	97.11	97.02	97.00	97.17	97.18	97.19	98.11	98.03	98.05
	KMNN	91.89	90.82	91.71	98.01	98.02	98.03	97.87	97.89	97.91	98.21	98.12	98.12

Table 5 Description of performance metrics

Test metric [10, 43]	Definition	Equation
Accuracy (α)	Computed by dividing all classes' correct identification by the dataset's total data points.	Accuracy (α) = $\frac{(T+)+(T-)}{(T+)+(T-)+(F+)+(F-)}$
Precision (ρ)	Computed by dividing the value of (T+) by the total of (T+) and (F+).	Precision (ρ) = $\frac{(T+)}{(T+)+(F+)}$
Recall (ξ)	Percentage of (T+) divided by the total of (T+) and (F-).	Recall (ξ) = $\frac{(T+)}{(T+)+(F-)}$
F-Score (F_s)	Precision and Recall harmonic mean is defined as F-score.	F-Score = 2 * $\frac{\xi * \rho}{\xi + \rho}$
False Positive Rate (F_+R)	Computed as the total number of (F+) divided by the sum of (T+) and (T-).	F_+R = $\frac{(F+)}{(T+)+(T-)}$
Area Under Curve (A_UC)	It is the trade-off between misclassification rate and F_+R. This is used to determine the best model for predicting abnormal data using all thresholds.	A_UC = $\frac{1}{2}(\frac{(T+)}{(T+)+(F+)} + \frac{(T-)}{(T-)+(F+)})$
True Positive Rate ($T+$)	The total data points identified as normal while they were actually normal.	
True Negative Rate ($T-$)	The total data points identified as abnormal while they were actual abnormal.	
False Positive Rate ($F+$)	The total data points identified as normal while they were actual abnormal.	
False Negative Rate ($F-$)	The total data points identified as abnormal while they were actually normal.	

Table 6 Performance summary of our proposed SEoT health monitoring framework

Data points	Algorithms	ρ (%)	ξ (%)	F_s (%)	α (%)	F_+R	A_UC (%)
1000	KMC	88.89	84.21	86.49	93.75	0.03	85.97
	FNN	82.35	82.35	82.35	92.5	0.04	78.43
	ANN	84.62	88.00	86.27	91.25	0.05	78.46
	KMNN	94.74	94.74	94.74	97.5	0.01	93.18
3000	KMC	83.72	75.79	79.56	90.75	0.04	79.88
	FNN	94.94	75.76	84.27	93	0.01	93.68
	ANN	90.32	73.68	81.16	93.5	0.02	88.65
	KMNN	93.06	94.37	93.71	97.75	0.01	91.64
5000	KMC	82.35	89.74	85.89	94.25	0.04	78.52
	FNN	93.67	82.22	87.57	94.75	0.01	92.16
	ANN	90.00	86.30	88.11	95.75	0.02	88.07
	KMNN	95.95	93.42	94.67	98	0.01	95.06
8000	KMC	91.11	86.32	88.65	94.75	0.02	88.72
	FNN	90.14	87.67	88.89	96	0.02	88.21
	ANN	91.55	90.28	90.91	96.75	0.02	89.87
	KMNN	96.00	96.00	96.00	98.5	0.01	95.11

description of each test metric with its factors is given in Table 5.

The clustering performance of the proposed SEoT health monitoring framework is evaluated. Table 6 illustrated the outcome of the experiment. The clustering performance is measured on all four different clustering approaches. The experiment has performed on different data points (1000, 3000, 5000, and 8000). It has been observed that the model's accuracy is improved while the data points increase. The accuracy results also illustrated that KMNN performance is better than the other three clustering approaches.

Another experiment was performed to determine the computation overhead in terms of time taken by the

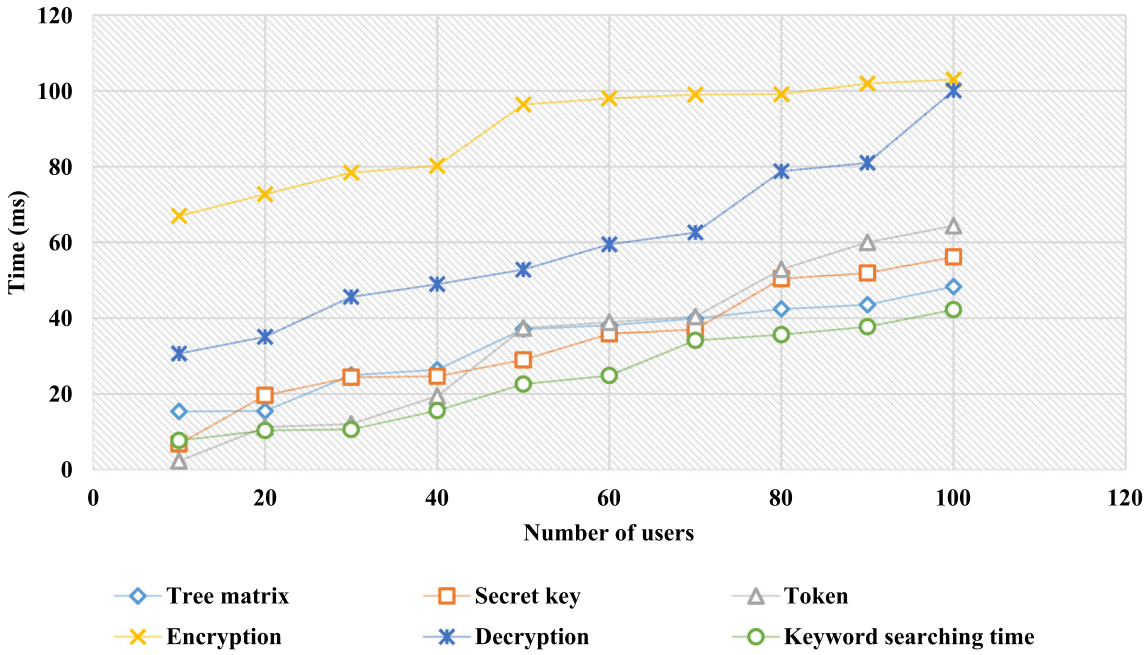

Fig. 9 Required time to perform the operations with respect to the number of users

proposed attribute-based encryption technique. This work implements the ABE encryption technique with an access policy to achieve data security and access control. Multiple operations are performed in the proposed ABE like tree matrix generation, secret key generation, token generation, encryption, decryption, and keyword searching. The time required to compute all these operations is calculated with respect to the number of users and data size. Figures 9 and 10 show the time taken to perform all these operations with respect to the number of users and data size, respectively. In Fig. 9, the graph's x-axis denotes the number of users, which ranges from 0 to 120 and the y-axis denotes the time. In Fig. 10 the graph's x-axis denotes the data size (in kb), which ranges from 0 to 1200 and the y-axis denotes the time. The achieved graphical result of both the figures illustrated that as the number of users/data size increases, the required time to perform the operation is also linearly increased.

5.1 Security analysis

In this section, we have discussed how the system will protect from different security attacks as explained below:

- *Access control* The proposed technique uses a searchable attribute-based encryption Algorithm based on the access policy. The codeword is used in this access control approach, which can give secret keys for different labels. The corresponding ciphertext can be accessed only if the user's attributes match the access control approach. The codeword of the attributes in the ciphertext cannot be retrieved if the user's fetched attribute does not match the access control approach.
- *Data confidentiality* In this approach, the patient data is encrypted with the secret key generated by the $MKEY\_GEN()$ and creates the encrypted index. After that, the ciphertext and encrypted index are sent to the cloud server. When the data user sends a request to the cloud server, the cloud server executes a search token using the keyword (attribute). As a result, the required information is fetched after maintaining data storage security.
- *Key security* Generally, no encryption techniques are used to deliver the user's key to the server in the attribute-based searchable encryption schemes. In this scheme, the user key is blindfolded with a codeword and each key location is stored to ensure the user key's security and secrecy. The server uses the key to establish if the user key attribute meets the search conditions, which results in user key leakage and loss of data confidentiality.
- *Anonymity* It shows that the patient data never reveal the patient's identity, or when a patient is communicating, the patient's identity should be kept secret. In this scheme, search tokens are generated anonymously with patient data. Also, the scheme provides non-likability with this search token so that no secret key is revealed throughout the process.
- *Data availability* In most attribute-based searchable schemes, the data availability chances get low because the ciphertext is saved on the cloud server. The

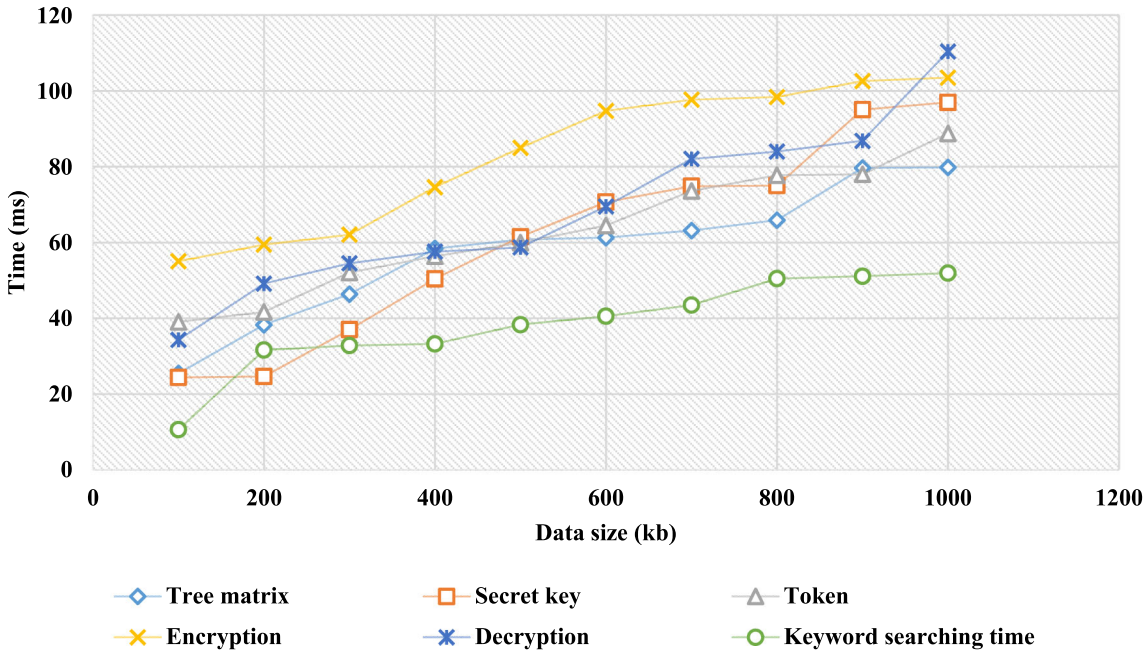

Fig. 10 Required time to perform the operations with respect to data size

keyword that acts as a trapdoor is provided to the cloud server whenever a keyword has to be searched. Now, for each file, a heuristic match is established using the trapdoor received by the cloud. If the match is successful, the keyword is present in the file. Finally, the cloud returns all files that successfully meet the search criteria to the user. Only the returned file has to be encrypted after getting the search results. However, in this scheme, the codeword is used for finding the search key which will track the document ID. This will increase the data availability chance high.

6 Conclusion

Smart healthcare systems provide a better opportunity to distribute the load of the overburdened traditional healthcare system. Most of the smart healthcare systems are based on cloud-based IoT technology. However, this technology's service latency rate is insufficient to cater to the demands of emergency, time-critical healthcare needs. So, the edge layer introduced between the IoT devices and the cloud layer called EoT manages to overcome a few limitations of a smart healthcare system. The SEoT framework for monitoring of health conditions of people has been proposed in this paper. The framework is aimed to predict or detect the chance of a diseased condition in a person by analyzing the deviation of observed bio-signal values from the usual or standard values. The framework detects the abnormal data received from the edge device. It provides secure access to sensitive data in the cloud. Four different clustering techniques have been used to detect abnormality in transmitted patient data. ABE technique with access policy is used to maintain the security of the patient data stored in the cloud. The outcome of the experiment KMNN clustering technique performed better than the other three algorithms. The algorithm maintains accuracy up to 98.5%. The efficiency of the proposed system can be enhanced by adding more edge devices at the edge layer. The future directions of this work can be done by adding blockchain technology to enhance the security and access control mechanism in the proposed framework.

Funding The authors did not receive support from any organization for the submitted work.

Data availability Not applicable.

Declarations

Conflict of interest There is no conflict of interest.

Ethical approval We did not use animals and Human participants in the study reported in this work.

Informed consent For this type of study informed consent is not required.

Consent for publication For this type of study consent for publication is not required.

References

1. Jigna, J.H., Sudeep, T.: An exhaustive survey on security and privacy issues in healthcare 4.0. Comput. Commun. **153**, 311–335 (2020)
2. Abdullah, L., Mazin, A.M., Ahmed, N.R., Seifedine, K., Thammarat, P., Karrar, H.A., Orawit, T.: Smart-contract aware ethereum and client-fog-cloud healthcare system. Sensors **21**(12), 4093 (2021)
3. Cao, K., Liu, Y., Meng, G., Sun, Q.: An overview on edge computing research. IEEE Access **8**, 85714–85728 (2020)
4. Ana, J.F., Joan, M.M., Josep, J.: Towards the decentralised cloud: survey on approaches and challenges for mobile, ad hoc, and edge computing. ACM Comput. Surv. (CSUR) **51**(6), 1–36 (2019)
5. Ola, S., Imad, E., Ayman, K., Ali, C.: Edge computing enabling the Internet of Things. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 603–608. IEEE (2015)
6. Zachary, W.L., Dharma, P.A.: Context-Aware Mobile Edge Computing in Vehicular Ad-Hoc Networks. In: 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1–7. IEEE (2018)
7. Mohammad P., Pedro, J.C., Rafael, D.T., Leandro do, C.M., Fatos, X., Angel, A.J.: Edge computing and IoT analytics for agile optimization in intelligent transportation systems. Energies, **14**(19), 6309 (2021)
8. Vaiyapuri, T., Binbusayyis, A., Varadarajan, V.: Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: A Systematic Review of Current and Future Trends. Int. J. Adv. Comput. Sci. Appl. **12**, 731–737 (2021)
9. Jaya Lakshmi, G., Ghonge, M., Obaid, A.J.: Cloud based IoT Smart Healthcare System for Remote Patient Monitoring. EAI Endorsed Trans. Pervasive Health Technol. **7**, 28 (2021)
10. Alabdulatif, A., Khalil, I., Yi, X., Guizani, M.: Secure edge of things for smart healthcare surveillance framework. IEEE Access **7**, 31010–31021 (2019)
11. Lakhan, A., Mastoi, Q.-U.-A., Elhoseny, M., Memon, M.S., Mohammed, M.A.: Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud. Enterprise Inform. Syst. **16**, 7 (2021). https://doi.org/10.1080/17517575.2021.1883122
12. Lakhan, A., Mohammed, M.A., Elhoseny, M., Alshehri, M.D., Abdulkareem, K.H.: Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system. Soft Comput. **26**, 6429–6442 (2022). https://doi.org/10.1007/s00500-022-07167-9
13. Lakhan, A., Mohammed, M.A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A., Wang, W.: Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE J. Biomed. Health Inform. (2022). https://doi.org/10.1109/JBHI.2022.3165945
14. Suhair, A., Stanislaw, P.R., Rajendra, K.R.: Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In: 2012 IEEE 28th international conference on data engineering workshops. pp. 143–146. IEEE (2012)
15. Lakhan, A., Mohammed, M.A., Rashid A.N., Kadry, S., Abdulkareem, K.H., Nedoma, J., Martinek, R., Razzak, I.: Restricted Boltzmann machine Assisted Secure Serverless Edge System for Internet of Medical Things. IEEE J. Biomed. Health Inform. (2022). https://doi.org/10.1109/JBHI.2022.3178660
16. Nasr Esfahani, M., Shahgholi Ghahfarokhi, B., Etemadi Borujeni, S.: End-to-end privacy preserving scheme for IoT-based healthcare systems. Wirel. Netw. **27**(6), 4009–4037 (2021)
17. Ke, W., Chien-Ming, C., Zhuoyu, T., Mohammad, S., Sachin, K., Saru, K.: Forward privacy preservation in IoT enabled Healthcare Systems. IEEE Trans. Indus. Inform. (2021)
18. Alzubi, J.A.: Blockchain-based Lamport Merkle digital signature. Comput. Commun. **170**, 200–208 (2021)
19. Itamir de Morais, B.F., Gibeon, A., Ramon Santos, M., Gustavo, G., Sávio Rennan, M.M.: An IoT-based healthcare platform for patients in ICU beds during the COVID-19 outbreak. IEEE Access **9**, 27262–27277 (2021)
20. Masud, M., Gaba, G.S., Choudhary, K., Hossain, M.S., Alhamid, M.F., Muhammad, G.: Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet Things J. **9**(4), 2649–2656 (2022). https://doi.org/10.1109/JIOT.2021.3080461
21. Castillo García, J.F., Ortiz, J.H., Ibrahim Khalaf, O., Valencia Hernández, A.D., Rodríguez Timaná, L.C.: Noninvasive prototype for type 2 diabetes detection. J. Healthc. Eng. **2021**, 8077665 (2021). https://doi.org/10.1155/2021/8077665
22. Rathee, G., Sharma, A., Saini, H., Kumar, R., Iqbal, R.: A hybrid framework for multimedia data processing in Iot-healthcare using blockchain technology. Multimedia Tools Appl. **79**(15), 9711–9733 (2020)
23. Sung, W.-T., Chiang, Y.-C.: Improved particle swarm optimization algorithm for android medical care IOT using modified parameters. J. Med. Syst. **36**(6), 3755–3763 (2012)
24. Yang, G., Xie, L., Mäntysalo, M., Zhou, X., Pang, Z., Da Li, X., Kao-Walter, S., Chen, Q., Zheng, L.-R.: A health-IoT platform based on the integration of intelligent packaging, unobtrusive biosensor, and intelligent medicine box. IEEE Trans. Indus. Inform. **10**(4), 2180–2191 (2014)
25. Aashay, G., Dhruv, D., Shubham, P., Vijayanand, R., Animesh, S., Vergin Raja, S.: IoT-based healthcare monitoring system for war soldiers using machine learning. Proc. Comput. Sci. **133**, 1005–1013 (2018)
26. Yang, Y., Zheng, X., Guo, W., Liu, X., Chang, V.: Privacy-preserving smart iot-based healthcare big data storage and self-adaptive access control system. Inform. Sci. **479**, 567–592 (2019)
27. Zgheib, R., Kristiansen, S., Conchon, E., Plageman, T., Goebel, V., Bastide, R.: A scalable semantic framework for IoT healthcare applications. J. Ambient Intell. Human. Comput. (2020). https://doi.org/10.1007/s12652-020-02136-2
28. Shreshth, T., Nipam, B., Sukhpal Singh, G., Mohsen, K., Rajesh Chand, A., Gurpreet Singh, W., Rajkumar, B.: HealthFog: an ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. Fut. Gener. Comput. Syst. **104**, 187–200 (2020)
29. Pournaghi, S.M., Bayat, M., Farjami, Y.: MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. J. Ambient Intell. Human. Comput. **11**, 4613–4641 (2020). https://doi.org/10.1007/s12652-020-01710-y
30. Sowjanya, K., Mou, D.: A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC. J. Inform. Secur. Appl. **54**, 102559 (2020)
31. Gagangeet, S.A., Anish, J.: A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring. IEEE J. Select. Areas Commun. **39**(2), 491–499 (2020)
32. Guo, X., Lin, H., Yulei, W., Peng, M.: A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems. Futur. Gener. Comput. Syst. **113**, 407–417 (2020)
33. Khushboo, S., Rudra, A., Sakshi, K.: An approach towards iot-based healthcare management system. In: Proceedings of the sixth international conference on mathematics and computing, pp. 345–356. Springer, New York (2021)

34. Umair Ullah, T., Haider, A., Lu, L., James, H., Muhammad, K., Waqar, A.: Energy-aware scheduling of streaming applications on edge-devices in iot-based healthcare. IEEE Trans. Green Commun. Netw. **5**(2), 803–815 (2021)
35. Singh, A., Chatterjee, K.: Securing smart healthcare system with edge computing. Comput. Secur. **108**, 102353 (2021)
36. Li, H., Yu, K., Liu, B., Feng, C., Qin, Z., Srivastava, G.: An efficient ciphertext-policy weighted attribute-based encryption for the Internet of health things. IEEE J. Biomed. Health Inform. **26**(5), 1949–1960 (2022). https://doi.org/10.1109/JBHI.2021.3075995
37. Vipin Kumar, R., Nikhil Kumar, R., Shubham, M., Bhavya Ahuja, G., Prayag, T., Amit Kumar, J., Shamim Hossain, M.: An edge ai-enabled iot healthcare monitoring system for smart cities. Comput. Electr. Eng. **96**, 107524 (2021)
38. Md Abdur, R., Shamim Hossain, M., Ahmad, J.S., Nabil, A.A., Mohammed, F.A.: A secure, private, and explainable ioht framework to support sustainable health monitoring in a smart city. Sustainab. Cities Soc. **72**, 103083 (2021)
39. Mehedi, M., Gurjot Singh, G., Karanjeet, C., Roobaea, A., Shamim Hossain, M.: A robust and lightweight secure access scheme for cloud based e-healthcare services. Peer-to-peer Netw. Appl. **14**(5), 3043–3057 (2021)
40. Taheri, R., Ghahramani, M., Javidan, R., Shojafar, M., Pooranian, Z., Conti, M.: Similarity-based Android malware detection using Hamming distance of static binary features. Futur. Gener. Comput. Syst. **105**, 230–247 (2020)
41. Oresti, B., Claudia, V., Rafael, G., Alejandro, S., Miguel, D., Juan, A.H.T., Sungyong, L., Hector, P., Ignacio, R.: Design, implementation and validation of a novel open framework for agile development of mobile health applications. Biomed. Eng. **14**(2), 1–20 (2015)
42. Banos, O., Garcia, R., Holgado-Terriza, J.A., Damas, M., Pomares, H., Rojas, I., Saez, A., Villalonga, C.: mHealthDroid: a novel framework for agile development of mobile health applications. In: International workshop on ambient assisted living, pp. 91–98. Springer, Cham (2014)
43. Singh, A., Chatterjee, K., Satapathy, S.C.: An edge based hybrid intrusion detection framework for mobile edge computing. Complex Intell. Syst. (2021). https://doi.org/10.1007/s40747-021-00498-4

Ashish Singh working as an Assistant Professor, School of Computer Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar, Odisha-751024. He has completed his Ph. D. in Computer Science & Engineering from National Institute of Technology Patna (Bihar) under Visvesvaraya Ph.D. Scheme for Electronics & IT Ministry of Electronics & Information Technology (MeitY) Government of India. He has completed M.Tech from National Institute of Technology Patna, Bihar, (India) in 2015. His research area includes cloud security, access control, trust management, healthcare security, edge computing, and network security.

Kakali Chatterjee is an Assistant Professor in Department of Computer Science and Engineering, National Institute of Technology Patna, Bihar, India. She has completed her Ph.D. from Delhi University (Delhi College of Engineering). She has done M.Tech from Centre for Development of Advanced Computing, a R&D and Academic centre of Govt. of India. She has published many research papers in LNCS (Springer) and reputed International Journals including Wireless Personal Communications (Springer), Information Security Journal: A Global Perspective (Taylor & Francis). She is working in the field of Information Security and cryptography.