Personal and Ubiquitous Computing
https://doi.org/10.1007/s00779-020-01475-3

ORIGINAL ARTICLE

# A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment

Samira Akhbarifar[1] · Hamid Haj Seyyed Javadi[2] · Amir Masoud Rahmani[1] · Mehdi Hosseinzadeh[3,4]

Received: 13 July 2020 / Accepted: 12 October 2020


**Abstract**
Internet of Things (IoT) and smart medical devices have improved the healthcare systems by enabling remote monitoring and screening of the patients' health conditions anywhere and anytime. Due to an unexpected and huge increasing in number of patients during coronavirus (novel COVID-19) pandemic, it is considerably indispensable to monitor patients' health condition continuously before any serious disorder or infection occur. According to transferring the huge volume of produced sensitive health data of patients who do not want their private medical information to be revealed, dealing with security issues of IoT data as a major concern and a challenging problem has remained yet. Encountering this challenge, in this paper, a remote health monitoring model that applies a lightweight block encryption method for provisioning security for health and medical data in cloud-based IoT environment is presented. In this model, the patients' health statuses are determined via predicting critical situations through data mining methods for analyzing their biological data sensed by smart medical IoT devices in which a lightweight secure block encryption technique is used to ensure the patients' sensitive data become protected. Lightweight block encryption methods have a crucial effective influence on this sort of systems due to the restricted resources in IoT platforms. Experimental outcomes show that K-star classification method achieves the best results among RF, MLP, SVM, and J48 classifiers, with accuracy of 95%, precision of 94.5%, recall of 93.5%, and f-score of 93.99%. Therefore, regarding the attained outcomes, the suggested model is successful in achieving an effective remote health monitoring model assisted by secure IoT data in cloud-based IoT platforms.

**Keywords** Internet of Things · Security · Block encryption · Health monitoring systems · Data mining

## 1 Introduction

In patients with novel COVID-19, there is an extraordinary rate of cardiovascular disease (CVD), and more than 7% of patients are involved with myocardial injury from the infection (22% of critically ill patients). The presence of novel COVID-19 increased the risk of death in CVD patients [1, 2]. Many already published and relevant articles show that diabetes, hypertension, and cholesterol levels have an ostensible relation to severity of novel COVID-19 [3]. Therefore, early diagnosis and prediction of serious chronic disease can widely contribute to reduce the heavy treatment burden on communities involving elderlies and disabled people who are commonly exposed to serious diseases such as CVD, heart disorders (HDs), hypertension (HTN), diabetes mellitus (DM), hypercholesterolemia (HCLS), or various infections such as novel COVID-19. In such situations, using computer-aided technologies has a positive significant role by providing accurate healthcare and medical decisions for recommending on-time and early essential treatments [4, 5].

In recent years, the growth of IoT and sensor technology related to wearable medical devices has enriched the patients' care quality through smart remote health monitoring systems [6]. Nowadays, the cloud-based IoT platforms are applied widely in smart remote health and medical monitoring systems

✉ Hamid Haj Seyyed Javadi
h.s.javadi@shahed.ac.ir

Mehdi Hosseinzadeh
hosseinzadeh.m@iums.ac.ir

[1] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2] Department of Mathematics and Computer Science, Shahed University, Tehran, Iran

[3] Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam

[4] Mental Health Research Center, Psychosocial Health Research Institue, Iran University of Medical Sciences, Tehran, Iran

Published online: 16 November 2020

[7, 8]. The combination of cloud and IoT has many benefits from resource management aspects such as resource distribution, powerful processing, avoiding from data fragmentation over various databases, and supporting user mobility in monitoring systems [9]. A modern remote health monitoring system in cloud-based IoT environment includes a context wherein the patients' biological data is transmitted and stored in clouds, and shared for the purpose of obtaining analytics from anywhere and anytime [10]. Due to the transferring of the patient's medical data through the IoT networks and storing them in the clouds, the confidentiality and security issues have become a crucial concern in these systems [11]. Therefore, applying data security techniques such as lightweight block encryption methods for constrained medical IoT resources seems to be an essential necessity for a safe and secure medical and health data management as one of the most important issues in constrained IoT platforms in critical systems [12, 13].

To obtain diagnostic information for predicting the patients' health abnormal changes, data mining methods are widely used in medical monitoring systems including classification and clustering methods, neural networks, and other approaches based on different machine learning techniques [14, 15].

In this paper, we propose a comprehensive lightweight secure remote health monitoring model that uses the benefits of both cloud and IoT technologies in which the patient can be remotely monitored by the medical teams for early diagnosing their critical conditions. To clear the details of our proposed model, some effective algorithms are developed to provide the functionality of our model. The main contributions of this paper are as follows:

1 Using a massive volume of acquired IoT sensor data as the main resource that conducts to apply the combination of cloud and IoT technologies.
2 Providing a lightweight block encryption method due to the constrained IoT resources used to forward the collected patient's critical medical data to the clouds in order to address confidentiality and security concerns.
3 Presenting a model for early disease diagnosis through data mining approaches including J48, support vector machine (SVM), multi-layer perceptron (MLP), K-star, and random forest (RF) which predict hypercholesterolemia (HCLS) and hypertension (HTN) and its severity level as HCLS complication, and also early predicting the heart disorders (HD) in the case of HCLS or HTN diagnosis.

The rest of this paper is organized as follows: In Section 2, a brief review on recent related works in this field is presented. Section 3 explains the offered secure health monitoring model in cloud-based IoT context. Section 4 provides detailed explanations about the suggested model that comprises of elements for data acquiring, securing and storing, data preprocessing, and data mining for disease diagnosis process through different data classification methods. In Section 5, the obtained experimental results through the statistical evaluation and also comparing them are presented. In Section 6, the conclusion and some future research directions in this area are provided.

## 2 Related work

This section reviews the recent papers in IoT and cloud-based remote health monitoring systems and predictive models for diagnosing the critical health status of patients. Three different aspects of remote health monitoring systems consist of (1) cloud-based, IoT-based, and cloud-based IoT frameworks and architectures; (2) applied data mining approaches in disease prediction systems; and (3) security solutions in IoT medical data management will be surveyed in these papers.

### 2.1 Remote health monitoring frameworks and architectures in IoT and clouds

A variety of frameworks, architectures, and schemas have been proposed for remote medical monitoring. Some of them were designed based on cloud technology and some others were introduced for IoT environments while a number of them were proposed in cloud-based IoT platforms to benefit both technologies. In the following, these aspects are surveyed in some recent papers:

- Cloud-based platforms: For instance, in [16], a cloud-based framework was offered that integrates meta-learning frameworks to order and select the finest predictive approach regarding the big data technologies for investigating the medical data. Also, a general-purpose framework was introduced in [17] for developing healthcare applications on cloud platforms. A strong instruction for achieving fast and elastic healthcare application on cloud platforms was presented in this study. Recently, in [18], a cloud-based 4-tier architecture was proposed that consists of four components comprising of data collection unit, data storage unit, analysis unit, and application presentation unit. The general supervised learning machine methods such as support vector machine (SVM), artificial neural network (ANN), random forest (RF), Naïve Bayes (NB), and decision tree (DT) techniques were used for early prediction of heart failures. Real-time prediction is the advantage of this paper. As well, in [19], a cloud-based framework was offered based on digital twin healthcare (CloudDTH) for observing, analyzing, and predicting the health status of aged people by wearable medical devices, for managing their personal health. Consequently, a new idea of digital twin healthcare (DTH) was suggested and implemented.
- IoT-based platforms: Several researches have been carried out on wearable IoT sensors and their applications in medical tracking approaches such as patient checking in IoT

platform through body area sensor networks which was developed in [20], through applying low powdered and lightweight sensors for continually monitoring the patient's status. The security necessities also were addressed in this work. Likewise, an IoT-based framework for tracking the patient's condition in ICU was introduced in [21]. Also, in [22], an ECG tracing technique in IoT context was designed, through wearable bio-sensors for direct medical data transition to the cloud storages. HTTP and MQTT protocols were used in this paper. Reliability is the main achievement of this work. Also, in [23], the methods for data mining including machine learning methods were applied such as SVM, DT, hidden Markov model (HMM), and Gaussian mixture model in IoT-based health monitoring systems for predicting abnormal conditions. In [24], a multipurpose IoT-based monitoring model was proposed to analyze the sensor data to predict the arthritis infections by IoT smart devices. Also, recently, in [25], an IoT-based schistosomiasis monitoring framework was proposed for more efficient disease prediction. Moreover, an IoT-based heart failure prediction and analysis model through machine learning methods was proposed in [26], and also, recently, in [27], a deep learning framework for prediction of heart disease was proposed for IoT context.

- Cloud-based IoT platforms: a variety of studies benefit the advantages of both technologies of cloud and IoT such as [9] that proposed a service-oriented IoT-based framework for unceasing patient condition tracking that used WBAN over smartphones to transfer medical data to the clouds. Experimental assessment regarding the lifetime of sensors, cost, and energy feeding revealed that the suggested framework considerably improves the standard WBANs. Also, in [28], an abstract framework for healthcare systems was suggested. In this paper, time-based mining process was used for obtaining the students' health data from the cloud sources to assess the students' health conditions. As well, in [29], a three-tiered architecture was presented which organized *n* for collecting, storing, and analyzing the huge volume of data supported by Apache HBase which was produced by wearable bio-sensors. The logistic regression method was used for predicting the heart diseases. The authors also proposed a cloud-based IoT mobile healthcare approach considering the security issues related to patient's sensitive medical data in [30]. They provided a classification method based on fuzzy rule–based neural classification approach. A scalable cloud-based architecture was offered in [31] for teleophthalmology in Internet of Medical Things (IoMT) for age-related macular degeneration (AMD) prediction considering the security requirements. Also, a hybrid intelligent approach was proposed for chronic kidney disease prediction in cloud-based IoT environment, in [32]. Recently, a medical monitoring scheme for cloud-based IoT platforms was proposed in [7] which applied a variety of classification methods for predicting a combination of diabetes mellitus, renal disorder, hypertension, and heart disease. Furthermore, in this paper, a medical/health service composition model extended by the authors in [33] was provided for the required recommendation that was produced by the offered system. Also, recently, in [8], a predictive diagnostic model was proposed for chronic kidney disease and its severity using IoT multimedia data in cloud-based IoT platform.

## 2.2 Data mining approaches in disease prediction systems

Generally, disease predication process via data investigation methods depends on data mining approaches. Generally, data mining includes the tasks of anomaly discovery, regression, and classification as the analytical mining approaches for training, and also, association rule learning, clustering, and data summarization, as the descriptive mining approaches for typifying the data in a distinct data set. All the stated approaches have been widely used for realizing the patterns of data in data mining tasks [34, 35]. In many papers such as [36–39], and also recently in [8, 40], the data mining and machine learning approaches were used for predicting a range of diseases. These approaches commonly include (1) statistical summarization of patients' medical data; (2) supervised learning such as regression analysis, neural networks, and automated classification that are extensively used in medical IoT systems; and (3) unsupervised learning, in case of absence of data class labels. Generally, in these papers, some assessment factors such as accuracy, precision, recall, and f-score have been considered for performance evaluation of disease prediction process.

Commonly, the most important challenge of data mining techniques may be the possible irrelevance of the discovered patterns, hence, to make them useful, they must be sound. For this purpose, the experts' assessments seem to be essential to achieve the precise results. Recently, employing the combined data mining methods effectively improves the classification process achievements [41].

## 2.3 Security solutions in IoT medical data management

In the surveyed papers, the security issues were considered in [7, 20, 30, 31], while in others they were not focused. Comparing to the analyzed papers, we aim to offer a secure remote health monitoring model in cloud-based IoT environment using data mining methods for early disease diagnosis which uses a lightweight block encryption method that is a proper solution for constrained medical IoT resources [42] which has not been focused in the studied papers. Therefore, the main contribution or advantage of our proposed model comparing to the previous papers is considering

confidentiality and security issues in an operative manner regarding the limitations in IoT resources. To depict this advantage, some comparing factors are considered in Table 1 including the following: presenting framework or architecture, applied technologies, security issues, applying lightweight block encryption methods in the studied papers comparing to our proposed model. As presented in Table 1, as well as providing a cloud-based IoT health monitoring model, a lightweight data encryption method is presented in our work whereas in others it was not considered.

## 3 Proposed secure health monitoring model in a cloud-based IoT environment

The proposed secure remote health monitoring model in a cloud-based IoT environment that benefits a lightweight block encryption method is represented in Fig. 1. Concerning the growth of hypercholesterolemia (HCLS) and hypertension (HTN) and consequently heart disease (HD), the combination of all these disorders is considered in this work. Therefore, the main objective of this paper is providing a secure health monitoring model for early diagnosis of the combination of HCLS, HTN, and HD based on predicting the critical patient's condition through these steps:

1 Remote medical monitoring via collecting the patient's biological data by medical IoT devices.
2 Applying a proposed lightweight block encryption method for providing the security and confidentiality on patient's medical data to provide secure medical IoT data.
3 Transferring the encrypted data to the clouds for disease prediction process.
4 Predicting the HCLS and detecting odd alterations in patients' blood cholesterol.
5 Predicting the risk of HTN and its severity levels, and then detecting HD in case of HTN diagnosis.
6 Forwarding the derived analytical outcomes of disease prediction process to the medical teams.

**Table 1** Comparing factors in the previous works vs. the proposed model

| Reference | Architecture/ framework | Applied technology | Security | Lightweight encryption method |
|---|---|---|---|---|
| [16] | ✓ | Cloud | ✗ | ✗ |
| [17] | ✓ | Cloud | ✗ | ✗ |
| [18] | ✓ | Cloud | ✗ | ✗ |
| [19] | ✓ | Cloud | ✗ | ✗ |
| [20] | ✓ | IoT | ✓ | ✗ |
| [21] | ✓ | IoT | ✗ | ✗ |
| [22] | ✓ | IoT | ✗ | ✗ |
| [23] | ✓ | IoT | ✗ | ✗ |
| [24] | ✓ | IoT | ✗ | ✗ |
| [25] | ✓ | IoT | ✗ | ✗ |
| [26] | ✓ | IoT | ✗ | ✗ |
| [27] | ✓ | IoT | ✗ | ✗ |
| [29] | ✓ | Cloud-based IoT | ✗ | ✗ |
| [28] | ✓ | Cloud-based IoT | ✗ | ✗ |
| [31] | ✓ | Cloud-based IoT | ✓ | ✗ |
| [30] | ✓ | Cloud-based IoT | ✓ | ✗ |
| [32] | ✓ | Cloud-based IoT | ✗ | ✗ |
| [9] | ✓ | Cloud-based IoT | ✗ | ✗ |
| [7] | ✓ | Cloud-based IoT | ✓ | ✗ |
| [36] | ✗ | Not mentioned | ✗ | ✗ |
| [35] | ✗ | Not mentioned | ✗ | ✗ |
| [34] | ✗ | Not mentioned | ✗ | ✗ |
| [43] | ✗ | Not mentioned | ✗ | ✗ |
| [38] | ✗ | Not mentioned | ✗ | ✗ |
| [44] | ✗ | Not mentioned | ✗ | ✗ |
| [37] | ✗ | Not mentioned | ✗ | ✗ |
| [39] | ✗ | Not mentioned | ✗ | ✗ |
| [8] | ✓ | Cloud-based IoT | ✗ | ✗ |
| Our proposed model | ✓ | Cloud-based IoT | ✓ | ✓ |

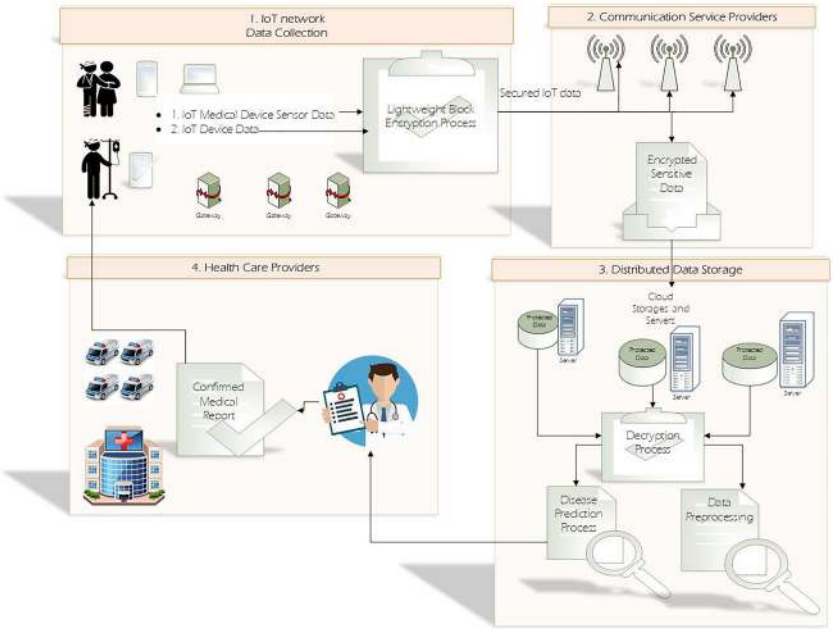


**Fig. 1** The proposed secure remote health monitoring model in cloud-based IoT environment

The proposed secure health monitoring model which is presented in Fig. 1 embraces four parts:

1 IoT network and data collection: This part comprises the network devices and medical IoT sensors and resources for sensing the patients' biological data to collect them. The collected data includes the patient's vital signs such as blood cholesterol, blood pressure, heart rate, and other required biological data sensed by the installed sensors on the patient's clothes or body over the body area network. Since the medical IoT sensor network devices are commonly found to be more at risk of security attacks comparing to other network devices, an element is designed for providing security necessities for secure IoT data. Before uploading the collected medical data to the clouds, a lightweight block encryption method is performed on the collected IoT data. This encryption method will be explained in detail in Section 4.2.
2 Communication service provider*:* This segment is responsible for transmitting the picked up patients' medical data to the cloud storage. This part must provide secret shares to transfer them to the cloud servers as a component of a distributed data storage structure.
3 Distributed data storage: The forwarded patients' medical data from the medical IoT sensors are stored in this part. Also distributed data storage segment deals with providing and giving services to the involved users that consist of doctors and healthcare providers. These services can be included in a facility for predicting the possible disease commonly through data mining methods. In our proposed secure health monitoring model, the combinations of three types of related disorders including hypercholesterolemia (HCLS), hypertension (HTN), and heart disorder (HD) are considered which will be explained in detail in Section 4.4.
4 Healthcare provider: This section comprises of doctors, hospitals, and emergency responders. The forwarded diagnosis results can be used by the doctors to check and confirm them for offering required medical recommendations to the patients.

The mentioned six steps for predicting the combination of HCLS, HTN, and HD are performed in four parts of the proposed model in Fig. 1, where the first and second steeps are done in IoT network and data collection component; the third step is performed after IoT network and data collection component, through communication service provider section. The fourth and fifth steps are executed in distributed data storage component. Finally, the last step is performed by healthcare provider section.

## 4 The proposed secure health monitoring model with a lightweight block encryption method for IoT data management

The offered model is responsible for required tasks to attain the aims of the proposed secure remote health monitoring model in cloud-based IoT context that utilizes a lightweight encryption method for provisioning security for IoT data management. These tasks consist of the following:

1 Acquiring the required data including patients' past clinical data and vital signs via body area network (BAN) and personal area network (PAN)

2 Securing the patient's medical data through a lightweight block encryption method
3 Transferring the encrypted data to the clouds for disease prediction process
4 Preprocessing the collected medical data
5 Predicting the combination of HCLS, HTN, HTN severity levels, and HD applying data mining methods
6 Forwarding the derived analytical outcomes of disease prediction process to the medical teams to confirm the diagnosis outcomes by the doctors

The process of performing the mentioned tasks is carried out through a workflow which is demonstrated in Fig. 2 via the Business Process Model and Notation (BPMN) [45]. In this workflow, some steps need to be performed in sequence, and some others are attached by exclusive operator which is displayed by "×" that signifies a forking point which is influenced by predicted disease type. Therefore, only one of the branches can be executed. The BPMN has also a parallel operator which is symbolized by "+" for simultaneous procedures which can be performed in a parallel manner. Another operator is the inclusive shown with "O" that specifies the choices for branch selection regarding the current state. The workflow graph of the suggested model is shown in Fig. 2 and the details are subsequently described.

In our proposed model, the mentioned tasks are performed through the provide workflow diagram presented in Fig. 2. As shown in Fig. 2, collecting IoT medical device sensor data and collecting IoT device data are performed in a parallel manner. Then, performing a lightweight data encryption on collected medical data, transferring secured medical data to the communication service providers, transferring and storing data in the clouds as distributed data storage, performing data decryption on secured data, data preprocessing, and finally predicting the combination of HCLS, HTN, and HD are performed sequentially. Then, based on diagnosis results and in detecting the abnormal condition, the diagnosis outcomes are confirmed by doctors and in case of emergency cases, a notification is sent to the patient and emergency providers are informed simultaneously. If emergency case is not determined, then diagnosis results are forwarded to the patient.

## 4.1 Data acquiring

In the proposed secure health monitoring model, based on Fig. 1 and the workflow in Fig. 2, different medical data as the required inputs are collected including the following:

1 IoT device data including patient's identification data and also some required past clinical data which must be entered by the patient.
2 IoT medical device sensor data such as blood cholesterol, systolic and diastolic blood pressure, heart rate, and other vital signs which are picked up via deployed IoT sensors on the patient's body or clothes.

Tables 2 and 3 display the details of required collected data that must be stored in the distributed data storages in clouds in our proposed secure health monitoring model.

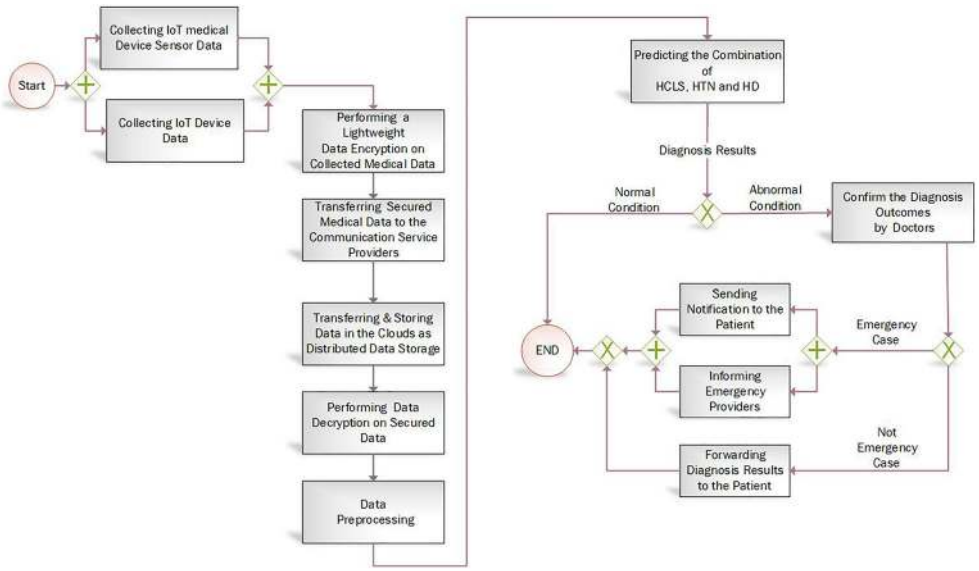


**Fig. 2** Workflow graph of the suggested secure health monitoring model

**Algorithm 1** presents the steps of collecting required IoT data for disease prediction process.

**Algorithm 1:** Data acquiring

**Input:** IoT device data , IoT medical device sensor data
**Output:** Required medical data

Begin
1. Enter the IoT device data including the identification data and the clinical data of the patient.
2. Collect the IoT medical device sensor data by sensors.
3. Transfer all the acquired medical data to the algorithm for lightweight block encryption process.

End.

### 4.2 Data security providing

Since security is one of the main issues in systems which was developed in the IoT context, for providing patient's anonymity, confidentiality, and security requirements, the sensitive patients' medical data is encrypted via performing algorithm 2. The complexity of the algorithm 2 is affected by the algorithm 3 that provides lightweight encryption. Therefore, the key performance parameters for evaluating the algorithm 3 are explained after presenting the related basic concepts in the following.

**Algorithm 2**: Data Encryption

**Input:** Acquired medical data
**Output:** Encrypted data

Begin
1. Read the acquired medical data provided by algorithm 1.
2. Encrypt acquired medical data via a lightweight block encryption method presented in algorithm 3.
3. Transfer encrypted medical data for storing in the distributed data storages.

End.

**Table 2** Details of required IoT device data in the proposed secure health monitoring model

| 1. IoT device data (patient's identification data) | 2. IoT device data (patient's clinical data) |
|---|---|
| • Patient's National id | • Weight |
| • Name | • Height |
| • Gender | • Smoker/Hookah |
| • Age | • Alcohol user |
| • Occupation | • Drug abuser |
| • Address | • Hypercholesterolemia (HCLS) history |
| • Mobile phone | • HLCS duration |
| | • HCLS control |
| | • Drug user |
| | • Hypertension (HTN) history |
| | • HTN duration |
| | • HTN control |

**Table 3** Details of required IoT medical device sensor data in the proposed secure health monitoring model

| IoT medical device sensor data |
|---|
| • Respiratory rate (RR) |
| • Heart rate (HR) |
| • Isolated systolic blood pressure (SBP) |
| • Isolated diastolic blood pressure (DBP) |
| • Oral temperature (OT) |
| • $O_2$ saturation (O2SAT) |
| • Cholesterol |
| • HDL cholesterol |
| • LDL cholesterol |
| • Triglycerides |

Generally, encryption plays a curtail role in making IoT systems secure. As an effective technique in block encryption methods, Substitution Box (S-Box) has an important impact [42, 43, 45, 46]. Due to the constrained resources of IoT devices, providing lightweight S-Boxes is a challenge. Algorithm 3 provides a key-dependent dynamic S-Box using Hyperelliptic curve.

To clear the applied main concepts in this paper, a brief explanation of the basic mathematical background required for developing the key-dependent dynamic S-Boxes is introduced. The suggested method relies on the idea of Hyperelliptic curve based on the presented definitions and related equations in Table 4.

Example 1 for Definition 1: Let $p = 11$. Over the finite field $F_p$, the equation $y^2 = x^5 + 2 \times x^2 + x + 3$ gives a Hyperelliptic curve of genus 2. The offered algorithm utilizes the divisor information in its computation steps.

Suppose that $H$ is a Hyperelliptic curve which is considered on a finite field $F_p$ and assume that $D_\alpha$ is a divisor of order "$n$." Given $D_\beta$, the Hyperelliptic Curve-Discrete-Logarithm-Problem (HCDLP) involves in attaining an integer $\lambda$, where $0 \le \lambda \le n-1$ , such that "$D_\beta = \lambda D_\alpha$" [48]. With $D_\beta$ and $D_\alpha$, it is impracticable to obtain the value of $\lambda$. In the proposed algorithm, the same features are used. The construction procedure is summarized in algorithm 3.

**Algorithm 3:** Proposed key-dependent dynamic S-Box Algorithm

**Input:** Finite prime field $\boldsymbol{F_p}$ , Equation of Hyperelliptic curve $C$ over $\boldsymbol{F_p}$, Key $\boldsymbol{\lambda}$
**Output**: Dynamic S-Box

1. Compute $\boldsymbol{D_\alpha} = \sum_{p \in c} \boldsymbol{m_p}\, \boldsymbol{P}$
2. Compute $\boldsymbol{D_\beta} = \boldsymbol{\lambda D_\alpha}$
3. Add $\boldsymbol{Z} = \boldsymbol{D_\alpha} + \boldsymbol{D_\beta} = \sum_{p \in c} \boldsymbol{m_p}\, \boldsymbol{P} + \sum_{p \in c} \boldsymbol{n_p}\, \boldsymbol{P} = \sum_{p \in c} (\boldsymbol{m_p} + \boldsymbol{n_p}) \boldsymbol{P} = (\boldsymbol{x_p} + \boldsymbol{y_p})$
4. Extract n bits of $\boldsymbol{x_p}$ and $\boldsymbol{y_p}$ to 16 words of 4-bits
5. Compute $\boldsymbol{x_p} \oplus \boldsymbol{y_p}$

Example 2: Let $p = 10^{34} + 1233$. Over the finite field $F_p$ and the equation $y^2 = x^5 + 2 \times x^2 + x + 3$, we choose two points $p_1$ and $p_1$ for $D_\alpha$ computation. Moreover, we generate a key for $D_\beta$. Finally, the S-Box is generated.

P1 = [28026955879377663890919100279076 40, 177427076027039770261572543921716]

P2 = [10000000000000000000000000000001231, 131261331295864003521648725458 5311]

Key = 23534739862384236842

S-Box = [1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0]

The performance of the suggested method for providing key-dependent dynamic S-Boxes is evaluated using the following criteria [49]:

a) Bijection: A bijection is defined as a one-to-one function over the components of two sets A and B, where each component of the set A is correlative to one component of the set B and exclusively vice versa. A bijective function $f: A \rightarrow B$ is considered a one-to-one relation of elements of a set like the $A$ into a set like the $B$.
b) Strict avalanche criteria (SAC): SAC is a function that fulfills the strict avalanche effect, if when a sight alteration is occurred in input bit, then a change will happen with a possibility of one-half in the output bit.
c) Nonlinearity: The generated S-Box should be extremely nonlinear which makes cryptanalysis procedure reasonably tough. Consider $a \times x + \delta$ as the assumed set of entire

**Table 4** Required mathematical definitions

| Definition | Equation |
|---|---|
| Definition 1: A Hyperelliptic curve $C$ of genus $g$ over finite field $F$ | $C: Y^2 + H(X)Y = F(X)$<br>Here, the $H(X)$ is considered a polynomial of the highest degree of $g$ and $F(X)$ is considered a monic polynomial of degree $2g + 1$ [47]. |
| Definition 2: Divisor $D$ is defined via a formal sum of points in $C$ | $D = \sum_{p \in c} m_p P, m_p \in Z$ |

affine functions that $a \in F_2^n$ and $\delta \in F_2$. Also, $b.F = b_1f_1 + \ldots + b_mf_m$ is considered a linear arrangement of the coordinate Boolean functions $f_i$ of $F$ that $b = (b_1, \ldots, b_m) \in F_2^n$ is non-zero. The nonlinear property (NL) for an assumed S-box is considered [50] as follows:

$NL(F) = \text{Min } d_H(b.F(x), a.x + \delta)$. The nonlinear property of the $n \times m$ S-Box is the smallest Hamming distance among the group of entire non-constant linear arrangements of component functions of $F$ besides the group of all related functions on $F_2^n$.

d) Algebraic degree: The Boolean function degree is the degree of the largest monomial in its algebraic normal form. The S-box should have high algebraic degree. An S-Box with low degree is susceptible to cryptanalytic attacks.

The proposed method is analytically evaluated using the mentioned assessment performance factors that will be discussed in Section 5.2. The evaluation results show that the offered algorithm is considerably an effective way to generate strong lightweight S-Boxes.

For legal admission to access the medical data by cloud services, the encrypted data is decrypted in clouds, which is described in algorithm 4.

**Algorithm 4:** Data Decryption Service (DDS)

**Input:** Encrypted medical data

**Output:** Decrypted data

Begin

1. Read the encrypted medical data that received form Algorithm 3.
2. Decrypt the data by cloud services.
3. Forward the decrypted medical data for storing in the cloud for authorized accessing.

End.

### 4.3 Data preprocessing

Generally, a preprocessing procedure should be used to clean the acquired data from noises in order to analyze them efficiently. As well, to cope with the occurred big data issues, the feature selection methods can effectively help the dimension reduction for simplifying the data mining process in disease prediction phase [35].

**Table 5** Combinations of the considered diseases

| Disease no. | Disease types |
|---|---|
| 1 | None |
| 2 | HCLS |
| 3 | HCLS, HTN1 |
| 4 | HCLS, HTN2 |
| 5 | HCLS, HTN3 |
| 6 | HCLS, HTN4 |
| 7 | HCLS, HD |
| 8 | HCLS, HTN1, HD |
| 9 | HCLS, HTN2, HD |
| 10 | HCLS, HTN3, HD |
| 11 | HCLS, HTN4, HD |

### 4.4 Disease prediction

The patients' data in cloud are analyzed via classification methods in this step. The core goal of this step is to predict the patients' health condition for diagnosing the HCLS and its complications including HTN and its severity levels, and HD through applying data mining methods on patients' medical data. Here, the main objective is that the patients can be categorized regarding their HCLS, HTN severity, and HD by classification methods. The various combinations of disorders comprising hypercholesterolemia (HCLS), hypertension (HTN) and its severity levels (HTN1: pre-hypertension; HTN2: stage I of hypertension; HTN3: stage II of hypertension; HTN4: critical stage of hypertension), and heart disease (HD) are presented in Table 5 [51].

Figure 3 illustrates the process of diagnosis phases regarding the combination of HCLS, HTN types, and HD through a workflow diagram [52, 53].

The process of disease prediction is described in algorithm 5 as follows:

**Algorithm 5:** prediction the diseases combination

**Input:** Decrypted medical data

**Output:** Diseases-type

Begin

1. Get the decrypted medical data.
2. Check Hypercholesterolemia considering
   (Gender, Age, Weight, HCLS history, HLCS duration, HCLS control, Drug user, Cholesterol, HDL Cholesterol, LDL Cholesterol, and Triglycerides).
3. If HCLS was not detected then Disease-type= "1. None"
   Else Check heart disease considering
   (Gender, Age, Weight, Height, Smoker/Hookah, Alcohol user,
   Drug abuser, Respiratory rate , Heart rate (HR),
   Isolated systolic blood pressure (SBP), Isolated diastolic blood pressure (DBP) and Drug user )
   AND
   Check hypertension Considering
   (Gender, Age, Weight, Height, Smoker/Hookah, Alcohol user,
   Drug abuser, HTN history, HTN duration, HTN control, Drug user,
   Isolated systolic blood pressure (SBP), Isolated diastolic blood pressure (DBP))
4. Case 1: If heart disease was not detected and hypertension was not detected then
   Disease-type= "2. HCLS"
5. Case 2: If heart disease was detected and hypertension was not detected then
   Disease-type= "2. HCL,HD"
6. Case 3: If heart disease was not detected and hypertension was detected then
   Check the HTN level considering
   (Isolated systolic blood pressure (SBP),
   Isolated diastolic blood pressure (DBP)

   Disease-type= "4. HCLS, HTN1" XOR

   Disease-type= "5. HCLS, HTN2" XOR

   Disease-type= "6. HCLS, HTN3" XOR

   Disease-type= "7. HCLS, HTN4"
7. Case 6: If heart disease was detected and hypertension was detected then
   Check the HTN level considering
   (Isolated systolic blood pressure (SBP),
   Isolated diastolic blood pressure (DBP)

   Disease-type= "8. HCLS, HTN1,HD" XOR

   Disease-type= "9. HCLS, HTN2,HD" XOR

   Disease-type= "10. HCLS, HTN3,HD" XOR

   Disease-type= "11. HCLS, HTN4,HD"
8. Transfer the Disease-type for Confirming by medical team..

End.

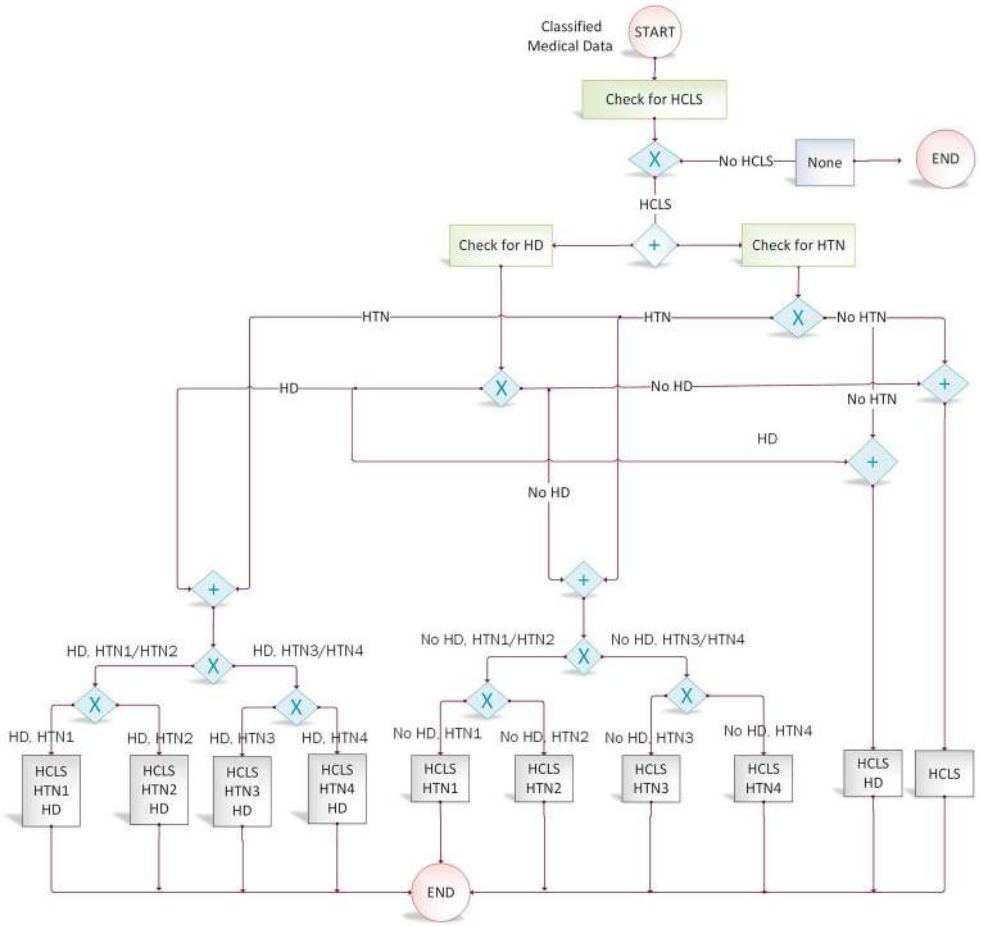


**Fig. 3.** The workflow of diagnosing the combinations of HCLS, HTN, and HD

To evaluate the effectiveness of disease prediction process, four factors containing accuracy, precision, recall, and f-score is computed. To obtain these factors, the confusion matrix is mostly used in machine learning classifiers [28]. The confusion matrix comprises the instances that include four sets consisting:

1 TP that is considered abnormal instances which have been classified correctly.
2 TN that is indicated as normal cases which have been classified correctly.
3 FP that is determined as abnormal instances that have been classified wrongly.
4 FN that is specified as normal cases that have been classified wrongly.

The assessment measures with their descriptions and related equations based on TP, TN, FP, and FN sets are as follows:

- Accuracy is obtained by $\frac{TP+TN}{TP+TN+FP+FN}$ that indicates the accuracy value of correctly predicted cases as healthy ones or abnormal.
- Precision is calculated via $\frac{TP}{TP+FP}$ that defines the positive predictive value that shows the portion of abnormal instances between all the samples.
- Recall is computed by $\frac{TP}{TP+FN}$ that indicates the portion of abnormal cases which have been obtained over all the abnormal samples.
- F-score is obtained by $2 \times \frac{Precision \times Recall}{Precision+Recall}$ that shows the performance via mixing precision and recall amounts.

In the proposed secure health monitoring model, some classification approaches are used over collected instances. As explained in Section 4.1, the required vital signs for all samples are gathered by IoT medical device sensors, and also, the identification and clinical data must be entered via IoT devices. The features of the main data set are illustrated in columns 1 to 4 in Table 6 which are required for prediction process in our scenario from all samples. The column 5 includes the resulted predicted diseases combinations including normal; only hypercholesterolemia; the combination of hypercholesterolemia and heart disease, the combination of hypercholesterolemia and hypertension; the combination of hypercholesterolemia, heart disease and hypertension [52, 53].

**Table 6** Main features for predicting hypercholesterolemia, hypertension, and heart disease

| 1. IoT Device Data | 2. IoT Device Data | 3.IoT Medical Devise Sensor Data | 4.IoT Medical Devise Sensor Data | 5.Diseases Diagnosis |
|---|---|---|---|---|
| Age (year) | Drug user<br>No: 0<br>Yes:1 | Cholesterol (CLS) (mg/dL.)<br>Normal: < 200 | Heart Rate (number/minute)<br>Normal: 60-100 | None |
| Gender (F/M) | Hypercholesterolemia (HCLS) history<br>No: 0<br>Yes:1 | HDL Cholesterol (mg/dL.)<br>Normal: ≥ 35 | O2 saturation O2SAT (percent)<br>Normal: ≥ 96 | HCLS |
| Weight (Kg.) | HCLS control<br>No: 0<br>Yes:1 | LDL Cholesterol (mg/dL.)<br>Normal: < 130 | Oral temperature (°C)<br>Normal: 37-38 | HCLS,HD |
| Height (cm) | HCLS duration (year) | Triglycerides (mg/dL.)<br>Normal: < 200 | | HCLS and HTN1/HTN2/ HTN3/HTN4 |
| Smoker=1/ Hookah=2/ Both=3 | Hypertension (HTN) history<br>No: 0<br>Yes:1 | Isolated systolic blood pressure<br>Normal: < 120<br>HTN1: 120-139<br>HTN2: 140-159<br>HTN3: 160-180<br>HTN4: ≥ 180 | | HCLS/HD and HTN1/HTN2/ HTN3/HTN4 |
| Alcohol user<br>No: 0<br>Yes:1 | HTN control<br>No: 0<br>Yes:1 | Isolated diastolic blood pressure<br>Normal: < 80<br>HTN1: 80-89<br>HTN2: 90-99<br>HTN3: 100- 110<br>HTN4 : ≥ 110 | | |
| Drug abuser<br>No: 0<br>Yes:1 | HCLS duration (year) | Respiratory rate (number/minute)<br>Normal: 8-12 | | |

## 5 Experimental outcomes and discussion

To assess the performance evaluation of the early disease detection process in our model, some usual classification approaches are used to classify the samples into eleven classes of different disease combinations indicated in Table 5. The tests were performed over the medical data of the healthy people and the patients. In our proposed secure health monitoring model, the patients' identification data and medical data were entered in the system by them, and since IoT provide a proper environment for constantly collecting vital data for health monitoring, we used the simulated IoT data for about 400 samples as the online dataset to achieve the analytic information.

The experiments on the proposed model are implemented in C# language and a series of computations has been conducted using the SageMath [54] for evaluating the performance of the proposed algorithm for providing key-dependent dynamic S-Boxes. The simulations have been done on the PC with an Intel Core i5, 3.33-GHz CPU, and 8-GB RAM.

The evaluation factors of f-score, accuracy, precision, and recall are obtained to check the effectiveness of the applied classifiers. The experiments carried out by Weka 3.6 revealed the classifiers' results obtained by different machine learning classification algorithms containing J48 [55], support vector machine (SVM) [56], multi-layer perceptron (MLP) [57], K-star [58], and random forest (RF) [59]. The test data file is processed applying training classification methods. For reducing the bias associated with random selection of samples for training, k-fold cross-validation method is applied that randomly divides the dataset into k distinct folds of closely identical size. Then, the classification is trained and tested k periods. In cross-validation procedure, the accuracy value shows the total number of correct classifications. In our experiments, the k-fold cross-validation method is applied with values of 1, 5, 10, 15, and 20 for k, for assessing the used classification methods. Also, the process of classification comprises the following k-fold cross-validation phases:

- K-fold dividing: The dataset is distributed into k-folds randomly over approximately the same number of instances.
- Labeling the classes: The instance choosing is indicated with the class labels.
- Training: In training step, the classifier for every disease classes over the normalized dataset is performed.
- Testing: A classifier is trained via k-1 of the k-folds for each subdataset, and then tested over the *k*th fold to obtain a cross-validation of its inaccuracy ratio.

Figures 4, 5, 6, and 7 show the resulted performance assessment factors over the testing set in applied classifiers that illustrates the different performance with different cross folds.

Regarding the experiments, the gained results for 10-fold cross-validation were the best outcomes and for 1-fold and 20-fold cross-validations, the results were the worst in all the classifiers. Overall, K-star showed the best performance and RF, MLP, SVM, and J48 respectively gained the most effective results after K-star. Thus, in prediction of the mentioned diseases in our proposed model, K-star classification method attained the highest performance comparing the other methods.

The obtained outcomes for 10-fold cross-validation as the best results are as follows:

- K-star: accuracy = 95%, precision = 94.5 %, recall = 93.5%, and f-score = 93.99%.
- RF: accuracy = 90%, precision = 87.5% and recall = 82.3% and f-score = 84.82%.
- MLP: accuracy = 84%, precision = 75% and recall = 70.5% and f-score = 72.68%.
- SVM: accuracy = 78%, precision = 70%, recall = 67.6%, and f-score = 68.77%.
- J48: accuracy = 63%, precision = 62%, recall = 62.4%, and f-score = 62.19%.

The gained results for evaluating the accuracy showed that 1-fold attained the lowest performance, and 5-fold, 15-fold, and 20-fold approximately showed about near performances. However, for assessing the precision, recall, and F-score factors, the experimental results revealed that 1-fold and 20-fold gained almost near performances as well as 5-fold and 20-fold that attained the same results approximately.

Some challenges including (1) data acquiring; (2) anonymity, confidentiality, and security issues; and (3) the predictive models for early disease diagnosis lead to the additional discussions that are explained in the following.

## 5.1 Data acquiring

In developed medical monitoring systems in IoT environments, IoT devices produce massive volumes of heterogeneous data that push to get the benefits of the cloud technology. Consequently, for cleaning the gathered data from anomalies and noises, a preprocessing step should be performed. Also, to cope with the big data problems [60, 61], the proper feature selection processes should be applied to reduce the dimensions for simplifying the process of classification. Therefore, addressing the related issues to collected data has a significant impact on effectiveness of classification methods.

## 5.2 Anonymity, confidentiality, and security issues

In this section, the effectiveness of the suggested method in algorithm 3 is evaluated through four criteria including bijection, strict avalanche criteria (SAC), nonlinearity, and algebraic degree. The experimental results are presented over the mentioned criteria.

The performance of the suggested method for providing key-dependent dynamic S-Boxes is evaluated using the following criteria [49]:

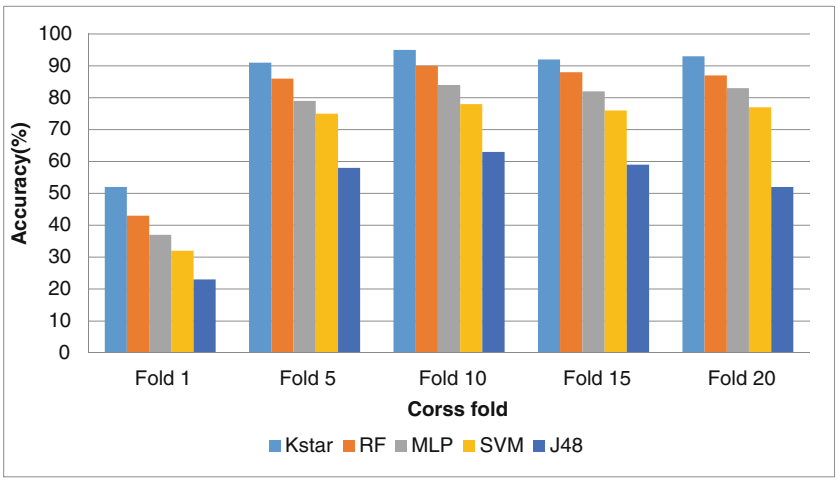


**Fig. 4** Accuracy for different folds

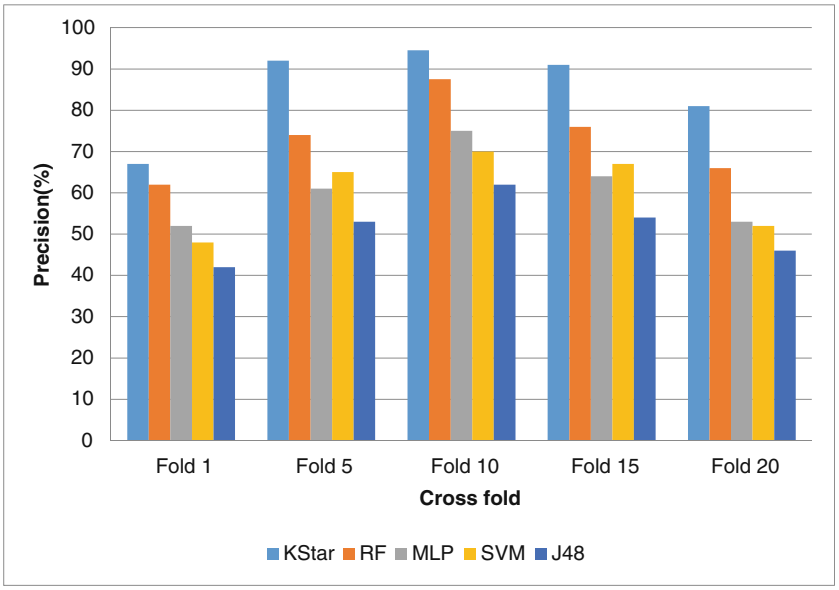


**Fig. 5** Precision for different folds

e Bijection: A bijection is defined as a one-to-one function over the components of two sets A and B, where each component of the set A is correlative to one component of the set B and exclusively vice versa. A bijective function $f: A \rightarrow B$ is considered as a one-to-one relation of elements of a set like the $A$ into a set like the $B$.

f Strict Avalanche Criteria (SAC): SAC is a function that fulfills the strict avalanche effect, if when a sight alteration is occurred in input bit, then a change will be happened with a possibility of one-half in the output bit.

g Nonlinearity: The generated S-Box should be extremely nonlinear which makes cryptanalysis procedure reasonably tough. Consider $a \times x + \delta$ as the assumed set of entire affine functions that $a \in F_2^n$ and $\delta \in F_2$. Also, $b.F = b_1 f_1 + \ldots + b_m f_m$ is considered a linear arrangement of the coordinate Boolean functions $f_i$ of $F$ that $b = (b_1, \ldots, b_m) \in F_2^n$ is non-zero. The nonlinear property (NL) for an assumed S-box is considered [50] as follows:

$NL(F) = \text{Min } d_H(b.F(x), a.x + \delta)$. The nonlinear property of the $n * m$ S-Box is the smallest Hamming distance among the group of entire non-constant linear arrangements of component functions of $F$ besides the group of all related functions on $F_2^n$.

h Algebraic degree: The Boolean function degree is the degree of the largest monomial in its algebraic normal form. The S-box should have high algebraic degree. An S-Box with low degree is susceptible to cryptanalytic attacks.

A series of computations has been conducted using the SageMath [54] for evaluating the performance of the suggested algorithm for providing key-dependent dynamic S-Boxes. In this research, it is attempted to compare the proposed method with PRESENT algorithm [62]. The

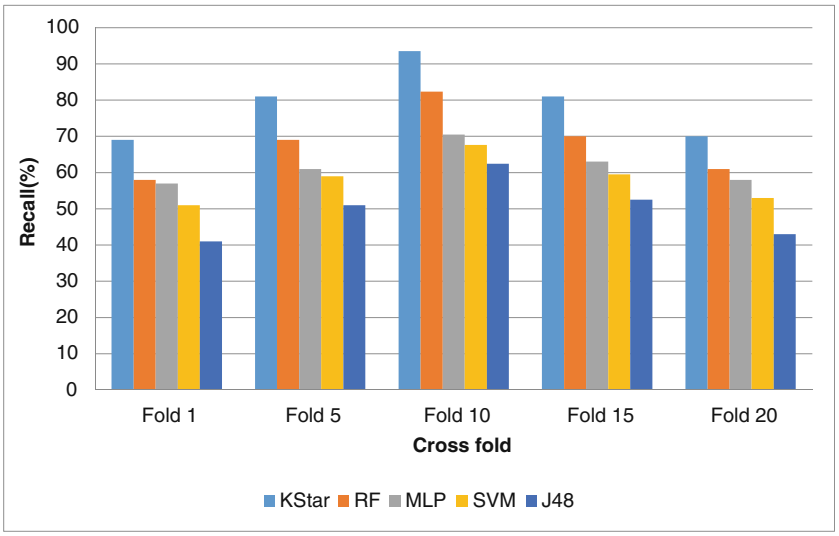


**Fig. 6** Recall for different folds

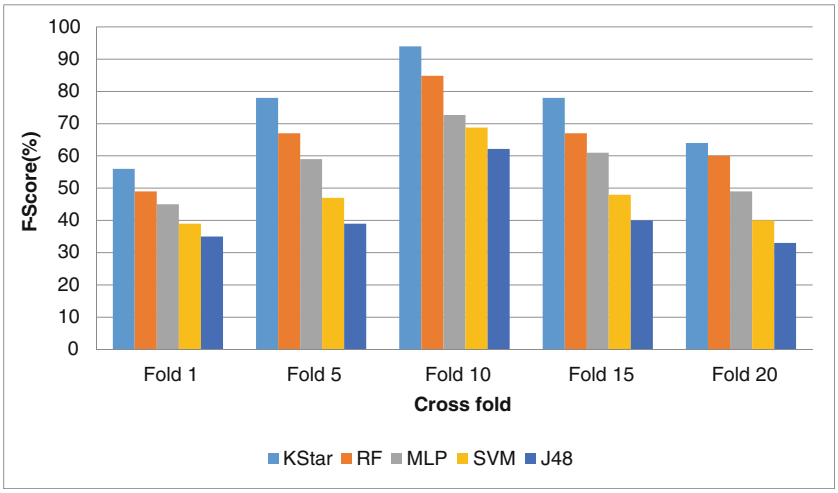


**Fig. 7** F-score for different folds

computations are made with 2 dissimilar keys and the obtained outcomes are presented in Table 7.

Regarding the gained outcomes, the abovementioned evaluation factors are discussed below:

a) Bijection: In the offered method for producing key-dependent dynamic S-Boxes, since the input vectors and output vectors are isomorphic, there is a one-to-one and onto representing from input to output. Therefore, the criterion of bijection is proper for the proposed method.
b) Strict Avalanche Criterion: In the proposed algorithm, minor alterations in the input vector cause a major variation in the output vector. The S-Boxes for the keys including 2 3 5 3 4 7 3 9 8 6 2 3 8 4 2 3 6 8 4 3 and 23534739862384236842 (one bit change) are:
[1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0], [1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0] and hence significantly different S-Boxes are produced. Therefore, strict avalanche criterion happened in the proposed dynamic key-dependent S-Box.
c) Nonlinearity: As the dynamic key-dependent S-Boxes are produced from the key in adequately random style, each S-Box possesses fairly high nonlinearity with a high probability of being complete. In [63], the authors proposed that nonlinearity has to be near the best recognized nonlinearity (i.e., $NL = 4$ attained by PRESENT S-Box). Thus, in this research, it is considered that $NL > 3$ for an S-Box to be categorized as the robust cryptography technique.
d) Algebraic Degree: As shown in Table 7, the algebraic degree of the proposed S-Box with the value of 4 is higher than PRESENT. Therefore, the proposed S-Box in this research can be classified as a strong solution against cryptanalytic attacks.

**Table 7** Evaluation results for the proposed S-Box method

| Algorithm | Nonlinearity | Min degree | Max degree |
|---|---|---|---|
| PRESENT | 4 | 2 | 3 |
| Proposed S-Box | 4 | 4 | 4 |

### 5.3 Predictive models for early disease diagnosis

As the influential tools for attaining accurate analytics in early disease diagnosis, data mining approaches are widely used by detecting the patterns that are not obviously visible [64, 65]. Commonly, a challenge of data mining process may be the possible worthlessness of the detected patterns, so, to make them beneficial, they must be reasonable. For this reason, generally, the experts' evaluations seem to be required to achieve the precise outcomes. Applying the combined classifiers can effectively increase the classification process success.

## 6 Conclusion and future work

Regarding the coronavirus (novel COVID-19) pandemic, the growing requirement for remote health monitoring has become a crucial concern in today's human lives considering the increasing aged population and people with threatening chronic diseases and high expenditures for taking care of all these patients. Real-time monitoring of patients and analyzing their health status can reveal the critical and abnormal conditions that meaningfully are valuable for early diagnosis of any threatening condition. The recent technologies such as medical IoT devices besides cloud resources contribute significantly in developing digital remote medical monitoring systems.

The core of this paper is proposing a remote health monitoring model which benefits secure IoT data management for early diagnosis of combinations of hypercholesterolemia,

hypertension, and heart disorder via data mining methods. Since the security and confidentiality issues are noticeably important in transferring patents' critical medical data through IoT networks and storing them in distributed cloud storages, regarding the limitations of resources in IoT environment, an effective lightweight block encryption method based on generating lightweight S-Boxes was also presented. Experimental outcomes show that K-star classification method with 95% accuracy, 94.5% precision, 93.5% recall, and 93.99% f-score provides the best results among RF MLP, SVM, and J48 classifiers for 10-fold cross-validation. Also, the outcomes showed that our proposed method for producing dynamic S-Boxes can be categorized as the robust cryptography technique based on the evauation factors including bijection, strict avalanche criterion, nonlinearity and algebraic degree. According to the gained experimental results, the proposed secure health monitoring model meets an effective development for remote medical monitoring to diagnose any threatening condition in patients besides preserving the confidentiality and security of their sensitive medical data.

As future work, we plan to implement our model in a real physical cloud-based IoT environment and also we will improve our existing model focusing the requirements in key-dependent S-Box designing that provides high security and throughput regarding the IoT resource limitations. We also aim to contribute the current restrictions in lightweight key-dependent dynamic S-Boxes providing a range of block encryption methods for supplementary studies in this direction. Also, we aim to focus on relation between chronic diseases such as heart disorder, hypertension, and hypocholesteremia and infection by novel COVID-19 in a real scenario.

## Compliance with ethical standards

**Conflict of interest** The authors declare that they have no conflict interest.

## References


1. Clerkin KJ, Fried JA, Raikhelkar J, Sayer G, Griffin JM, Masoumi A, Jain SS, Burkhoff D, Kumaraiah D, Rabbani LR, Schwartz A, Uriel N (2020) COVID-19 and cardiovascular disease. *Circulation* 141:1648–1655
2. Bansal M (2020) "Cardiovascular disease and COVID-19," Diabetes & Metabolic Syndrome: Clin Res Rev
3. Zaki N, Alashwal H, Ibrahim S (2020) Association of hypertension, diabetes, stroke, cancer, kidney disease, and high-cholesterol with COVID-19 disease severity and fatality: A systematic review. *Diabetes Metab Syndr Clin Res Rev* 14:1133–1142
4. Ting DSW, Carin L, Dzau V, Wong TY (2020) Digital technology and COVID-19. *Nat Med* 26:459–461
5. Vaishya R, Javaid M, Khan IH, Haleem A (2020) "Artificial intelligence (AI) applications for COVID-19 pandemic," Diabetes Metab Syndrome: Clin Res Rev
6. Al-Turjman F (2020) Intelligence and security in big 5G-oriented IoNT: an overview. *Futur Gener Comput Syst* 102:357–368
7. Asghari P, Rahmani AM, Javadi HHS (2019) A medical monitoring scheme and health-medical service composition model in cloud-based IoT platform. *Trans Emerg Telecommun Technol* 30: e3637
8. Hosseinzadeh M, Koohpayehzadeh J, Bali AO, Asghari P, Souri A, Mazaherinezhad A, et al. (2020) "A diagnostic prediction model for chronic kidney disease in internet of things platform," Multimedia Tools Appl pp. 1-18
9. Ghanavati S, Abawajy JH, Izadi D, Alelaiwi AA (2017) Cloud-assisted IoT-based health status monitoring framework. *Clust Comput* 20:1843–1853
10. Darwish A, Hassanien AE, Elhoseny M, Sangaiah AK, Muhammad K (2019) The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. *J Ambient Intell Humaniz Comput* 10:4151–4166
11. Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiquzzaman M (2018) Privacyprotector: privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun Mag* 56:163–168
12. Chaudhry SA, Yahya K, Al-Turjman F, Yang M-H (2020) "A secure and reliable device access control scheme for IoT based sensor cloud systems." IEEE Access
13. Chaudhry SA, Alhakami H, Baz A, Al-Turjman F (2020) Securing demand response management: a certificate based access control in smart grid edge computing infrastructure. IEEE Access
14. Ismail A, Shehab A, El-Henawy I (2019) Healthcare analysis in smart big data analytics: reviews, challenges and recommendations. In security in smart cities: models, applications, and challenges. Springer, Cham, pp 27–45
15. Safdar S, Zafar S, Zafar N, Khan NF (2018) Machine learning based decision support systems (DSS) for heart disease diagnosis: a review. *Artif Intell Rev* 50:597–623
16. Vukićević M, Radovanović S, Milovanović M, Minović M (2014) Cloud based metalearning system for predictive modeling of biomedical data. Sci World J 2014
17. Verma P, Sood SK (2018) Cloud-centric IoT based disease diagnosis healthcare framework. *J Parallel Distrib Comput* 116:27–38
18. Ahmed MR, Mahmud SH, Hossin MA, Jahan H, Noori SRH (2018) "A cloud based four-tier architecture for early detection of heart disease with machine learning algorithms," in 2018 IEEE 4th International Conference on Computer and Communications (ICCC), , pp. 1951-1955
19. Liu Y, Zhang L, Yang Y, Zhou L, Ren L, Wang F, Liu R, Pang Z, Deen MJ (2019) A novel cloud-based framework for the elderly healthcare services using digital twin. *IEEE Access* 7:49088–49101
20. Gope P, Hwang T (2016) BSN-Care: a secure IoT-based modern healthcare system using body sensor network. *IEEE Sensors J* 16: 1368–1376
21. Bhatia M, Sood SK (2016) Temporal informative analysis in smart-ICU monitoring: M-HealthCare perspective. *J Med Syst* 40:190
22. Yang Z, Zhou Q, Lei L, Zheng K, Xiang W (2016) An IoT-cloud based wearable ECG monitoring system for smart healthcare. *J Med Syst* 40:286
23. Banaee H, Ahmed M, Loutfi A (2013) Data mining for wearable sensors in health monitoring systems: a review of recent trends and challenges. *Sensors* 13:17472–17500
24. Parthasarathy P, Vivekanandan S (2018) A typical IoT architecture-based regular monitoring of arthritis disease using time wrapping algorithm. *Int J Comput Appl*:1–11
25. Kassé B, Gueye B, Diallo M, Santatra F, Elbiaze H (2019) IoT based schistosomiasis monitoring for more efficient disease prediction and control model. In 2019 IEEE Sensors Applications Symposium (SAS) pp 1–6
26. Ganesan M, Sivakumar N (2019) "IoT based heart disease prediction and diagnosis model for healthcare using machine learning

models," in 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), pp. 1-5
27. Nguyen T-H, Nguyen T-N, Nguyen T-T (2020) "A deep learning framework for heart disease classification in an IoTs-based system." in A Handbook of Internet of Things in Biomedical and Cyber Physical System. ed: Springer, pp. 217-244
28. Verma P, Sood SK, Kalra S (2018) Cloud-centric IoT based student healthcare monitoring framework. *J Ambient Intell Humaniz Comput* 9:1293–1309
29. Kumar PM, Gandhi UD (2018) A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. *Comput Electr Eng* 65:222–235
30. Kumar PM, Lokesh S, Varatharajan R, Babu GC, Parthasarathy P (2018) Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. *Futur Gener Comput Syst* 86:527–534
31. Das A, Rad P, Choo K-KR, Nouhi B, Lish J, Martel J (2018) Distributed machine learning cloud teleophthalmology IoT for predicting AMD disease progression. Future Gen Comp Syst 93: 486–498
32. Abdelaziz A, Salama AS, Riad A, Mahmoud AN (2019) A machine learning model for predicting of chronic kidney disease based internet of things and cloud computing in smart cities.In Security in Smart Cities: Models, Applications, and Challenges. Springer, Cham, pp 93–114
33. Asghari P, Rahmani AM, Javadi HHS (2020) Privacy-aware cloud service composition based on QoS optimization in Internet of Things. J Ambient Intell Human Comput 1-26
34. Rahimi B, Vimarlund V (2007) Methods to evaluate health information systems in healthcare settings: a literature review. *J Med Syst* 31:397–432
35. Li D, Park HW, Ishag MIM, Batbaatar E, Ryu KH (2016) "Design and partial implementation of health care system for disease detection and behavior analysis by using DM techniques," in Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14th Intl C, pp. 781-786
36. Sharma S, Chen K, Sheth A (2018) Toward practical privacy-preserving analytics for iot and cloud-based healthcare systems. *IEEE Internet Comput* 22:42–51
37. Samuel OW, Asogbon GM, Sangaiah AK, Fang P, Li G (2017) An integrated decision support system based on ANN and Fuzzy_AHP for heart failure risk prediction. *Expert Syst Appl* 68:163–172
38. Malathi D, Logesh R, Subramaniyaswamy V, Vijayakumar V, Sangaiah AK (2019) Hybrid reasoning-based privacy-aware disease prediction support system. *Comput Electr Eng* 73:114–127
39. Manogaran G, Varatharajan R, Priyan M (2018) Hybrid recommendation system for heart disease diagnosis based on multiple kernel learning with adaptive neuro-fuzzy inference system. *Multimed Tools Appl* 77:4379–4399
40. Souri A, Ghafour MY, Ahmed AM, Safara F, Yamini A, Hoseyninezhad M (2020) A new machine learning-based healthcare monitoring model for student's condition diagnosis in Internet of Things environment. Soft Computing 24:17111–17121
41. Reddy GT, Reddy MPK, Lakshmanna K, Rajput DS, Kaluri R, Srivastava G (2020) Hybrid genetic algorithm and a fuzzy logic classifier for heart disease diagnosis. *Evol Intel* 13:185–196
42. Ali Z, Chaudhry SA, Ramzan MS, Al-Turjman F (2020) Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles. *IEEE Access* 8:43711–43724
43. Duan L, Street WN, Xu E (2011) Healthcare information systems: data mining methods in the creation of a clinical recommender system. *EnterInform Syst* 5:169–181
44. Nilashi M, Ibrahim O, Ahmadi H, Shahmoradi L, Farahmand M (2018) A hybrid intelligent system for the prediction of Parkinson's disease progression using machine learning techniques. *Biocybern Biomed Eng* 38:1–15
45. Geiger M, Harrer S, Lenhard J, Wirtz G (2018) BPMN 2.0: the state of support and implementation. *Futur Gener Comput Syst* 80:250–262
46. Ara T, Shah PG, Prabhakar M (2018) "Dynamic key dependent S-Box for symmetric encryption for IoT devices," in 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC), pp. 1-5
47. Koblitz N (2012) Algebraic aspects of cryptography vol. 3. Springer Science & Business Media, Berlin
48. Van Tilborg HC, Jajodia S (2014) Encyclopedia of cryptography and security. Springer Science & Business Media, Berlin
49. Daemen J, Rijmen V (2013) The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media
50. Isa H, Jamil N, Z'aba MR (2016) Construction of cryptographically strong S-Boxes inspired by bee waggle dance. *N Gener Comput* 34: 221–238
51. Chang C-D, Wang C-C, Jiang BC (2011) Using data mining techniques for multi-diseases prediction modeling of hypertension and hyperlipidemia by common risk factors. *Expert Syst Appl* 38:5507–5513
52. Mohan S, Thirumalai C, Srivastava G (2019) Effective heart disease prediction using hybrid machine learning techniques. *IEEE Access* 7:81542–81554
53. Lee BJ (2019) Prediction model of hypercholesterolemia using body fat mass based on machine learning. *J Converg Cult Technol* 5:413–420
54. Stein WA (2012) Sage mathematics software (Version 4.8), ed. The Sage development team, England
55. Kaur G, Chhabra A (2014) Improved J48 classification algorithm for the prediction of diabetes. Int J Comp Appl 98(22)
56. Suykens JA, Vandewalle J (1999) Least squares support vector machine classifiers. *Neural Process Lett* 9:293–300
57. Pal SK, Mitra S (1992) Multilayer perceptron, fuzzy sets, and classification. *IEEE Trans Neural Netw* 3:683–697
58. Mahmood DY, Hussein MA (2013) Intrusion detection system based on K-star classifier and feature set reduction. *Int Organ Sci Res J Comput Eng* 15:107–112
59. Liaw A, Wiener M (2002) Classification and regression by randomForest. *R News* 2:18–22
60. Shadroo S, Rahmani AM (2018) Systematic survey of big data and data mining in internet of things. *Comput Netw* 139:19–47
61. Prakash A, Navya N, Natarajan J (2018) "Big Data preprocessing for modern world: opportunities and challenges," in International Conference on Intelligent Data Communication Technologies and Internet of Things, pp. 335-343
62. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, et al. (2007) "PRESENT: an ultra-lightweight block cipher." in International workshop on cryptographic hardware and embedded systems, pp. 450-466
63. Carlet C (2011) On known and new differentially uniform functions. In Australasian Conference on Information Security and Privacy. Springer, Berlin, Heidelberg, pp 1–15
64. Fki Z, Ammar B, Ayed MB (2018) "Machine learning with Internet of Things data for risk prediction: application in ESRD," in 2018 12th International Conference on Research Challenges in Information Science (RCIS), pp. 1-6
65. Palani D, Venkatalakshmi K (2019) An IoT based predictive modelling for predicting lung cancer using fuzzy cluster based segmentation and classification. *J Med Syst* 43:21