IoT ENABLED HEALTHCARE MONITORING SYSTEM USING CONVOLUTIONAL NEURAL NETWORK

Gasim Alandjani
Department of Computer Science and Engineering, Yanbu Industrial College, Kingdom of Saudi Arabia
E-Mail: alandjanig@rcyci.edu.sa

ABSTRACT

Recent development in the Internet of Things (IoT) based smart mobile healthcare monitoring provides better dimensionalities and smart services. The introduction of IoT-based wearable sensor devices circumvents the death of millions of people with regular monitoring and better treatments. This type of monitoring system also increases the data and it is necessary to store the data in any service-provided platform and the cloud is one among them all. The security of data is also a concern while transmitting the data. Further, the prediction of diseases from the collected data is also an intricate process. To address these issues, we propose a novel deep learning-based approach known as Convolutional Neural network-based disease prediction, and the security of the data stored in the cloud can be acquired by the Rivest-Shamir-Adleman (RSA) cryptography algorithm. The performance of our proposed work is analyzed with some state-of-art works. The comparative study shows that the proposed work achieves better security and also the prediction accuracy of our proposed is higher.

Keywords: IoT devices, smart applications, healthcare monitoring, cloud, RSA, convolutional neural network.

1. INTRODUCTION

Health care monitoring is an important task to monitor for most deadly diseases and also for an elderly person. It is a type of collection of health-related data from patients and covers most of the issues of major public health importance [1]. It includes a geographic spreadsheet, cost, numbers and trends, and health impact. Moreover, it includes a correlation between the components such as health problems and respective determinants based on our understanding. The main purpose of monitoring the health of the public is to provide better treatment at the right time [2]. Thus the physicians of recent years carry the vast medical archives at their fingertips. These are achieved by modern technology which includes smart and artificial intelligence-based applications. Of these smart technologies, IoT is one and most widely used and also provides better results.

IoT is basically used to connect many devices without any human interventions [3]. Hence this technology significantly reduces manpower and is also available at the cheapest rate. The main advantages of using IoT in healthcare monitoring are that it can be accessed remotely without any extra cost. This circumvents the staying of patients in the hospital for a long time for the treatment of chronic diseases. It also mitigates the space of the healthcare industries and enables patient interaction in delivering solutions for diseases [4].

Another reason why we are choosing IoT instead of all other technologies for healthcare monitoring is that the devices are easily portable that is most of the devices are in a wearable format. This device monitors the health of the patients or normal people by tracking the heart rate, blood pressure, and more relies on the type of disease [5]. Moreover, these devices are tuned to remind the blood pressure deviations, blood pressure, calorie count, and more. Therefore the utilization of IoT-based smart devices to monitor health issues can reduce the death rate to a great extent. However, the classification of diseases from the collected data from the IoT-enabled device is important to provide better treatment. In context with this many researchers utilized artificial intelligence-based approaches however, the prediction accuracy is low are yet to be optimized. Hence we utilized CNN-based disease prediction and for secured data storage RSA based authentication process is used. The key factors of the proposed work are listed below:

- The data are collected from wearable IoT-based sensor devices and checked with the normal data. Henceforth the data are forwarded to the cloud platform and for secured communications of data; we have utilized RSA based cryptography approach.
- The disease prediction from the collected data is performed by using the CNN approach which effectively predicts the diseases from the gathered data.

The rest of the work is organized accordingly: the relevant works are reviewed in section 2. The proposed secured disease prediction is elucidated in section 3. The justification of the proposed work is made in section 4. The work is concluded in section 5.

2. RELATED WORKS

Rajan Jeyaraj *et al.* [6] suggested a deep neural network (DNN) for IoT-based healthcare systems via a patient monitoring system. For signal measurement, an important intelligent sensor provides an advanced electronic component. The higher electronics component by intelligent sensor designs smart monitor. The prediction accuracies of four physiological signals are for validating the Smart-Monitor system. The experimental results

VOL. 18, NO. 3, FEBRUARY 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

provided 97.2% average accuracy with the accurate and reliable monitoring system. The encryption model is poor.

The deep learning (DL) model was introduced by Wu *et al*. [7] for real-time health monitoring in IoT. The valuable information was extracted via different deep-learning algorithms. The athletes' conditions are properly investigated via the DL model. By regarding different statistical-based performance measures, the cross-validation test evaluates the DL performance in healthcare monitoring. Among the athletes, dreadful diseases like cancer, heart disease, and brain tumors were diagnosed by considering effective tools but the accuracy is less.

Kaur *et al*. [8] introduced a random forest (RF) based healthcare monitoring system in IoT. Depending upon empirical and historic information placed on the cloud, the recommendations are driven by allowing this system. By using several input attributes linked to a specific disease, the diseases such as liver disorders, dermatology, thyroid, diabetes, breast cancer, and heart diseases were predicted. The huge feature dimensionality makes higher computational complexities.

Godi *et al*. [9] introduced the machine learning (ML) technique for IoT healthcare monitoring systems. In medical and health domains, several novel enhancements with drastically improving models are used in IoT. Regularly and periodically monitor the patient's health-related data. An advanced automation system was designed by Machine learning (ML) methods integrated with E-Healthcare Monitoring System (EHMS) was introduced. For proper diagnosis, the decisions making and proper monitoring model were designed.

3. PROPOSED FRAMEWORK

Figure-1 describes the architecture of the proposed framework. From remote areas, medical IoT device such as implanted and wearable IoT devices collects the data. The medical IoT device collected data, UCI repository datasets, and the health-related data of patients are fed to the cloud database. From this cloud database, the patient's data are collected and the secured information's stored and followed by the different diseases predicted.

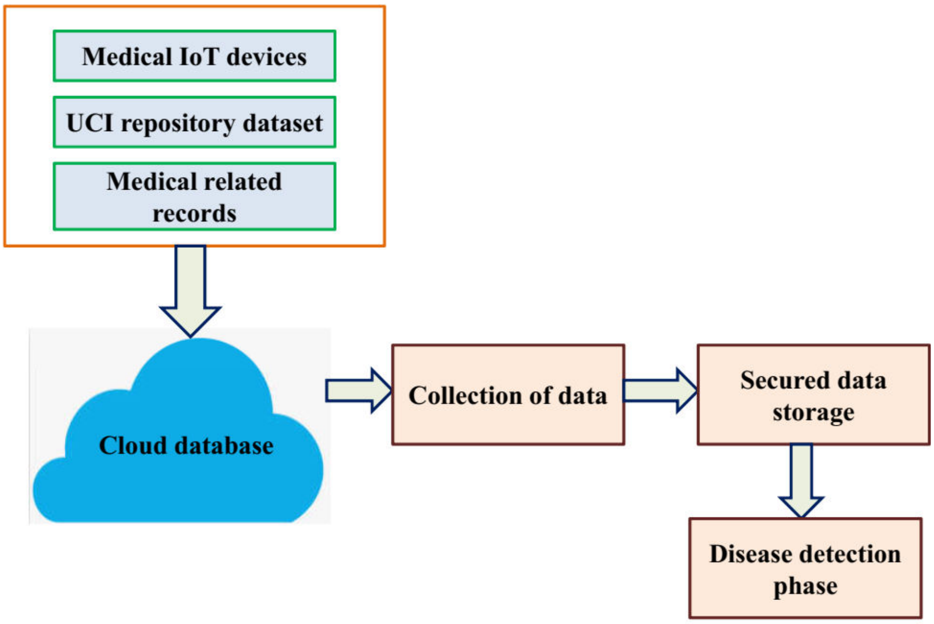

Figure-1. Proposed system framework.

3.1 Collection of Data

The proposed approach deems three different types of data and these data are collected from the sensors that are installed in the wearable IoT devices. The patients used to wear these devices on their bodies and collect the details at regular interval. Inside the device itself, the checking of details takes place with the normal data and if the data deviates from the normal details it will alert the patients as well as the physician. For the transmission of data to the cloud, our proposed approach utilizes 5G networks.

3.2 Secured Data Storage

The decision-making or prediction of diseases might have been carried out by considering three types of data: (i) data that are gathered from individual patients from the remote area for the analysis, (ii) UCI repository dataset, and (iii) collecting the medical history of the patients from the hospitals. Storing all those datasets requires enormous space and handling them is also a crucial task. Data security is an intricate task while handling these types of data. For security, we proposed a novel RSA [10] based encryption and decryption and elucidated it in the following section.

3.2.1 Rivest-Shamir-Adleman (RSA) cryptography algorithm

RSA is public-key cryptography [11] commonly used for security purposes and our proposed work is utilized for secured medical data stored in the cloud platform. It is usually used to provide an effective authentication scheme over insecure communications. While performing the authentication scheme the server generates the public key which is used for the authentication. This public key is sent to the user along with the private key and thus forms a digital signature for the secured communications. The created signature is forwarded to the user and thus validates with the server's public key as shown in Figure-2.

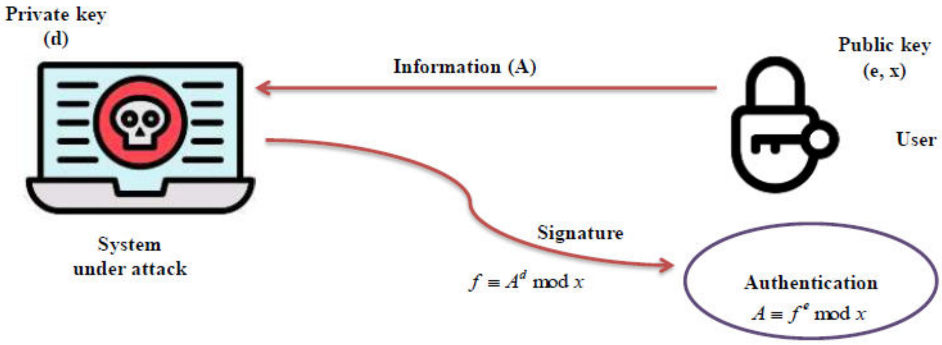

Figure-2. Authentication process utilizing our proposed RSA approach.

The public key-based authentication is performed by generating a suitable pair of public keys known as (x, e) and private keys (x, d). The value of x can be obtained from the sum of two distinct prime numbers and the estimation of e and d for any form of data known as A. However, it must justify the following conditions such that, $A \equiv \left(A^d\right)^e \bmod x \equiv \left(A^e\right)^d \bmod A$. Data A can be authenticated by appending the signature f to the data by the server and forwarding the pair. Generation f is performed by the server from the A along with its private key and using $f \equiv A^d \bmod x$. Those who know the public key can access the data through the verification process with the aid of $A \equiv f^e \bmod x$.

3.3 Disease Prediction Phase

In this study, the convolutional neural network (CNN) is used for disease identification. The mammal brain's deep structure inspires deep learning. The CNN is the most important deep network, which involves a different number of convolution, pooling, and fully connected layers. Figure-3 explains the structure of CNN.

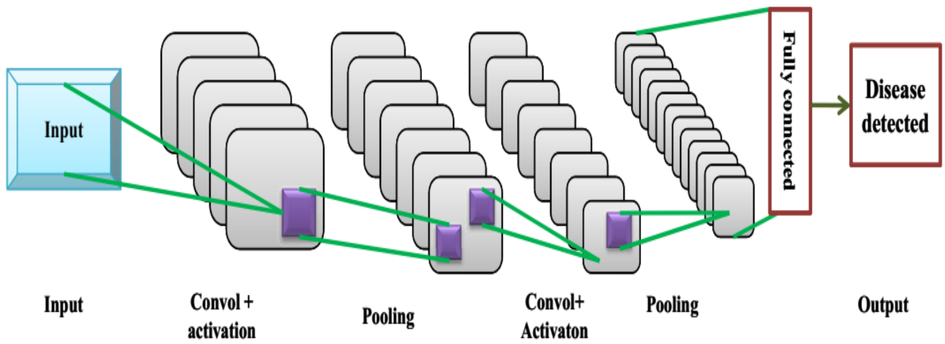

Figure-3. Disease detection using CNN.

3.3.1 Convolutional layer

The feature vector is the output and inputs of subsequent convolutional layers, which includes more convolutional layers [12]. The generated feature map $\left(m^*\right)$ depth and the input convolve these filters.

$$CON_j^{(L)} = A_j^{(L)} + \sum_{k=1}^{b_j^{(L-1)}} I_{j,k}^{(L-1)} * CON_k^{(L)} \quad (1)$$

Where, $CON_k^{(L)}$ denotes the L^{th} output convolutional layer and has feature maps. The kernel size

$b*b$ and the convolution filter is $I_{j,k}^{(L-1)}$ with the bias matrix $A_j^{(L)}$.

3.3.2 Pooling layer

From the previous convolution layer, extract the feature maps and the dimensionality is reduced. Perform the pooling operation among the feature maps and mask. The maximum, sum, and average pooling are the subsampling methods. This study utilizes max pooling for disease prediction.

3.3.3 Fully connected layers

One or more hidden layers with the traditional feed-forward network are the fully connected layer. The below equation express the softmax activation function from the output layer.

$$X_j^{(L)} = F\left(Y_j^{(L)}\right) \tag{2}$$

Where,

$$Y_j^{(L)} = \sum_{j=1}^{n_j^{(L-1)}} W_{j,k}^{(L)} Y_j^{(L-1)} \tag{3}$$

In order to represent disease prediction output, tune the weights $W_{j,k}^{(L)}$ and the transfer function is *F*. Initialize the CNN training next to find the disease detection output [13]. The stochastic gradient descent method performs training. Finally, CNN effectively detects diseases.

4. EXPERIMENTAL INVESTIGATIONS AND DISCUSSIONS

JAVA programming is used as the implementation platform. This section discusses the experimental analysis of the proposed framework using various state-of-art comparisons and different performance metrics such as specificity, sensitivity, and accuracy.

$$Specificity = \frac{FN}{TN + FP} \tag{4}$$

$$Sensitivity = \frac{TP}{TP + FN} \tag{5}$$

$$Accuracy = \frac{TP + TN}{TN + FP + FN + TP} \tag{6}$$

The true positive and negative classes are TP and TN also FP are FN the false positive and negative classes.

The state-of-art results for disease prediction performance are tabulated in Table-1. The methods including DNN [6], DL [7], RF [8], ML [9] and proposed methods are used for state-of-art comparison. The accuracy, sensitivity and specificity of the proposed method are 94%, 92% and 93% respectively, which is superior to existing methods.

Table-1. State-of-art comparison for disease prediction.

Techniques	Performance measures		
	Accuracy	Specificity	Sensitivity
DNN [6]	93%	90%	92%
DL [7]	90%	89%	88%
RF [8]	67%	60%	62%
ML [9]	70%	79%	63%
Proposed	94%	92%	93%

The validation of the proposed secured communication between the user and the server can be performed and analyzed. Then the outcomes are compared with state-of-art works such as DNN [6], DL [6], RF [8], and ML [9]. A comparative study is performed based on the public key generation time, private key generation time, and security analyses. Figure-4 illustrates the comparative study based on the generation duration of the public key in the second. From the graphical representation, we can observe that the time of our proposed approach is low which is equal to 56 seconds. Meanwhile, other approaches DNN [6], DL [6], RF [8], and ML [9] generate the public key with the duration of 123 sec, 98 sec, 158 sec, and 107 sec respectively.

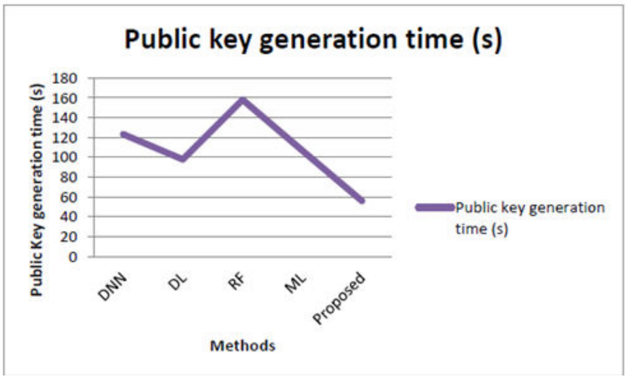

Figure-4. Graphical representation of comparative study based on the public key generation time.

The private key generation time-based comparative study is illustrated in Figure-5. From the figure, we observed that the proposed approach takes time a duration of 23 sec. The other state-of-art works such as DNN [6], DL [6], RF [8], and ML [9] take time duration of 78 sec, 86 sec, 48 sec, and 67 sec respectively. The comparative study based on the security level is delineated in figure 6. The security level of our proposed approach is 97% and other existing approaches DNN [6], DL [6], RF [8], and ML [9] achieve 83%, 92%, 87%, and 89% respectively.

VOL. 18, NO. 3, FEBRUARY 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

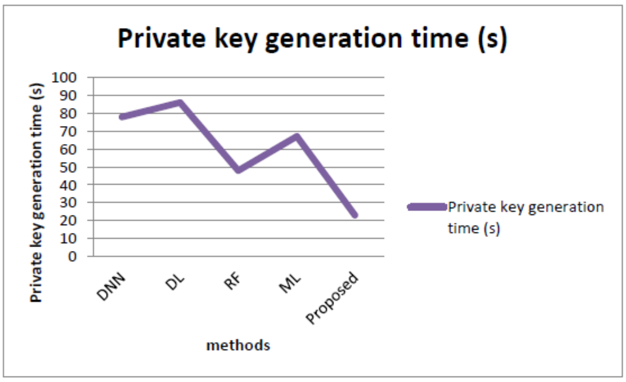

Figure-5. Graphical representation of comparative study based on the private key generation time.

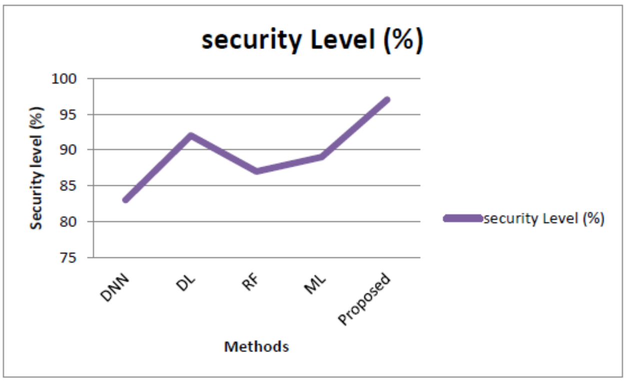

Figure-6. Graphical representation of comparative study based on the private key generation time.

5. CONCLUSIONS

This article presented IoT enabled healthcare monitoring system using CNN. The Rivest-Shamir-Adleman (RSA) cryptography algorithm can be used to ensure the security of data stored in the cloud. The performance of our proposed work is compared to some cutting-edge works. According to the comparative study, the proposed work achieves better security and has higher prediction accuracy. The proposed model demonstrated 94%, 92%, and 93%accuracy, sensitivity, and specificity to existing DNN, DL, RF, and ML techniques.

REFERENCES

[1] Valsalan, Prajoona, Tariq Ahmed Barham Baomar, and Ali Hussain Omar Baabood. IoT based health monitoring system. Journal of critical reviews 7, no. 4 (2020): 739-743.

[2] Yun Sung-Hwa, Dong-Hyun Kim and Jong-Tae Park. 2009. Design and implementation of u-healthcare monitoring system based on SOA. The Journal of Korean Institute of Communications and Information Sciences. 34(10B): 988-993.

[3] Chaudhury Shreyaasha, Debasmita Paul, Ruptirtha Mukherjee and Siddhartha Haldar. 2017. Internet of Thing based healthcare monitoring system. In 2017 8th annual industrial automation and electromechanical engineering conference (IEMECON), pp. 346-349. IEEE.

[4] Acharya Anand D. and Shital N. Patil. 2020. IoT based health care monitoring kit. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 363-368. IEEE.

[5] Saha H. N., Paul D., Chaudhury S., Haldar S. and Mukherjee R. 2017, October. Internet of Thing based healthcare monitoring system. In 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 531-535). IEEE.

[6] Rajan Jeyaraj P. and Nadar E. R. S. 2019. Smart-monitor: patient monitoring system for IoT-based healthcare system using deep learning. IETE Journal of Research. pp. 1-8.

[7] Wu Xingdong, Chao Liu, Lijun Wang and Muhammad Bilal. 2021. Internet of things-enabled real-time health monitoring system using deep learning. Neural Computing and Applications. 1-12.

[8] Kaur P., Kumar R. and Kumar M. 2019. A healthcare monitoring system using random forest and internet of things (IoT). Multimedia Tools and Applications. 78(14): 19905-19916.

[9] Godi B., Viswanadham S., Muttipati A. S., Samantray O. P. and Gadiraju S. R. 2020, March. E-healthcare monitoring system using IoT with machine learning approaches. In 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA) (pp. 1-5). IEEE.

[10] Dharminder D., Mishra D. and Li X. 2020. Construction of RSA-based authentication scheme in authorized access to healthcare services. Journal of medical systems. 44(1): 1-9.

[11] Pellegrini Andrea, Valeria Bertacco and Todd Austin. 2010. Fault-based attack of RSA authentication. In 2010 Design, Automation and Test in Europe Conference & Exhibition (DATE 2010), pp. 855-860. IEEE.

[12] Abiyev R. H. and Ma'aita H. M. K. S. 2018. Deep convolutional neural networks for chest diseases detection. Journal of healthcare engineering.

[13] Tm P., Pranathi A., Sai Ashritha K., Chittaragi N. B. and Koolagudi S. G. 2018. August. Tomato leaf disease detection using convolutional neural networks. In 2018 eleventh international conference on contemporary computing (IC3) (pp. 1-5). IEEE.