International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Data Transmission in Healthcare Internet of Things Using Bayesian Deep Q Neural Network with Privacy Preservation Authentication Scheme

M. Lorate Shiny[1,2], Kalpana Murugan[3*], Nagaraj Ramrao[4]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract: The integration of the Internet of Things (IoT) in the healthcare industry has led to the development of efficient IoT-based healthcare systems for real-time patient monitoring, with the ability to store and process large amounts of data. However, the sharing of sensitive patient information, such as health status and device usage, over the cloud raises security concerns. To address these issues, cryptographic methods and deep learning models have been used to provide secure data transmission and anomaly detection. In this paper, a privacy-preserving deep learning model called the Bayesian Deep Q neural network (BDQNN) with Ciphertext-attribute based policy encryption (CP-ABPE) has been proposed to protect transmitted data from external threats and reduce communication overhead in an IoT-based healthcare system. The proposed model was evaluated through simulation experiments and demonstrated superior performance compared to traditional methods, with an accuracy of 98.3%, sensitivity of 94.2%, specificity of 96.9%, precision of 95.9%, communication overhead of 68.1%, encryption time of 59.4ms, and decryption time of 60.2ms.

Keywords: *Healthcare security, Internet of Things, Deep learning, Privacy-preserving, cipher text, attribute encryption, deep Q network.*

1. Introduction

Due to the reason of many people living with chronic diseases and the aging population, there is exerting pressure on the healthcare system around the world [1]. There is a need for the healthcare staff to support the healthcare industry efficiently and effectively, which helps in critical emergencies. The transformation from traditional healthcare to digital form helps to improve the quality of service and assists medical professionals. This provides a spectrum of a solution called 'eHealth' or digital health [2]. For instance, digital technologies such as sensors [3], internet facilities, and relevant advanced software are used for real-time monitoring of sick-person's in their residency. The medicinal-sensors capture the factual-period medical data of the patient and send these medical data to the hospital medical centers which are stored as electronic health records of the patients used by the doctors for analysis. Mostly, Artificial Intelligence (AI) based approaches are used for this decision system. Based on these analyzed outcomes, the treatment is decided, and the emergencies are avoided by providing the necessary medical assistance by medical professionals. The major aim of these advanced medical services which allows sick-persons living self-sufficiently by getting improved medical caring services at resident itself. The health-related data are remotely monitored [4] which provides countless advancement in medical identification and handling.

The internet of things (IoT) used IP-based communication to connect to the internet with sensors and devices. For instance, the IoT in the healthcare sector obtained remote monitoring, treatment, diagnosis, and prevention [5].

The people who used these sensors are furnished with Radio Frequency Identification (RFID) tags, and actuators to monitor the status. Using the IoT applications, the RFID tags, and the patients' medical devices are located, read, recognized, and monitored [6]. The dynamic nature of IoT connects the healthcare industry [7] to connect the object to devices, patients to machines, patients to doctors, mobiles to patients, sensors to mobiles, and tags to readers for processing. This remote monitoring through healthcare IoT opens new supports in the suggestion of health care services and improves patient eminence of life. Though, while transferring stored medical records in public available IT environment, safety and secrecy remain considered the foremost issues [8, 9]. The patient personnel medical data are to be confidential in transmission and storage. Data protection is defined by the security objectives such as data integrity, data secrecy, user authentication, and so on. Hence, while designing the

[1]*Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil,Virudhunagar,Tamilnadu, India-626126.*
[2]*Department of Electronics and Communication Engineering, Dayananda Sagar University, Bangalore-560068.*
ORCID ID: 0000-0002-1368-6369
[3*]*Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Virudhunagar, Tamilnadu-626126, India.*
ORCID ID: 0000-0002-5121-0468
[4]*Mohan Babu University, Andhra Pradesh-517102*
ORCID ID: 0000-0003-2542-5999
** Corresponding Author Email: drmkalpanaece@gmail.com*

healthcare support system, the security objectives are a major consideration and the security mechanism called cryptographic operations is implemented to obtain the objectives.

In an IoT environment, the safety and secrecy of patient medical records will be most important concept [10]. Data security is achieved by storing and transferring the data securely which ensures authenticity, validity, and integrity. Data privacy is achieved while accessing the data by authorized individuals [11]. Based on the demands, needs, and purposes, protection strategies are developed with IoT devices that improve the sick-person fitness and secure the information. The next-generation systems, IoT devices are affected by known and unknown attacks [12]. Data transferred from the IoT over then storage on cloud techniques and handling is altered at several points. The conventional system using signature-based encryption and Machine learning approaches is not sufficient to deal with the frequently occurring unknown attacks. Deep learning (DL) can be used in recent years to visualize the communication network to recognize normal data with higher accuracy [13]. Moreover, training time is the major concern for DL-based models compared to existing approaches. Hence, it is needed to develop a novel approach that reduces the training time, and computation overhead without compromising the detection accuracy with improved security. With these objectives, this paper contributes the following:

- Novel healthcare secure system has been proposed using deep learning with a privacy preservation approach. The Bayesian-optimized Deep Q neural network may be deployed on process of the patient data for real-time monitoring which will reduce the network traffic.
- Further, the patient data has been secured while transmission by adopting Ciphertext-attribute based policy encryption (CP-ABPE) which has been proposed in our previous research work.
- The efficiency of the proposed DL-based security system has been evaluated and compared with the conventional tactics in relations of computational overhead, data-accuracy, sensitivity over data, data specifications, data-precision, encryption, decryption time.

The research paper's organized as follows: Section 2 defines the related work on healthcare IoT privacy preservation approaches. Section 3 creates proposed system model through DL-based privacy preservation methods. Section 4 describes as well as compares the investigational outcomes of between proposed, existing approaches. Section 5 concludes the proposed model with its future exploration guidelines.

2. Related Work

It discussed associated privacy preservation approaches for healthcare IoT Meniawy et al., [14] developed an authentication system that enables the sensors and medical professionals to validate every one other to share the crypto-graphical keyword which is deployed in data security. This protocol assigns the patient to the doctors to control the patient data access dynamically. Using the ProVerif protocol, the security analysis is performed and ensures forward secrecy, mutual authentication, and secret key establishment. Deebak et al., [15] proposed a protected and unidentified biometric-centered validation system as SAB USA. This system ensures the security of the healthcare industry. The analyzed results show that a genuine user does not act as an imposter to access patient data. Privacy preservation disease prediction (PPDP) [16] was developed by Zhang et al [16] This encrypts the data efficiently and stores sick-person health data over the cloud-based server for processing. Using single-layer perceptron neural network, the prediction model was trained.

Wang et al., [17] proposed IoT based healthcare system that supports signature-based methods with verifiability and forwards privacy using the trapdoor permutation function. It distinguishes the newly added data and past search data which ensures forward secrecy. They also developed a multi-keyword search verification system to verify the correctness of the system. Kathamuthu et al., [18] proposed Deep Q learning with a confidentiality maintenance model to defend the transmitted datasets from external threats. This method also reduces the network traffic on processing the data which reduces the communication cost and error. Compared to the existing approaches, it secured 93.74% of accuracy, 92% of sensitivity, 92.1% of specificity, 67.08% communication overhead, 58.72ms of encryption time, and 62.72ms of decryption time.

Ahamad et al., [19] developed an advanced ML-based data privacy-preserving model in the cloud. It consists of two stages such as sanitization and data re-establishment. The sanitization process generates ideal data-key using the cross Meta heuristic Jaya and shark smell optimization methodology. The parameters including modification degree, the ratio of preservation information, and as hiding ratio are delivered by the multi-objective function which generates the optimal key. Veeramakali et al., [20] developed optimal DL with secure blockchain-based intelligent healthcare IoT. It includes three processes such as secured transaction, encryption, and diagnosis. This model secured 93.68% of accuracy with a data-sensitivity as 92.75% with a data-specificity of 91.42%.

Hui et al., [21] proposed varying fractional chaotic systems that utilized the synchronization between the

fractional drive system and response system. Using the N shift encryption process, the data signals are encrypted and decrypted. Abirami and Banu [22] developed distributed secured model using crypto DNN. This model has been processed by the cloud server, data center, web server, and cloud agent. Using the crypto DNN cloud security, personalization attacks are handled which obtained a 10% of packet loss reduction and 5% increased response time compared to traditional approaches. Zhang et al., [23] designed hierarchical fuzzy NN for privacy preservation. It consists of two approaches to learning the parameters. Two optimization algorithms are used to process the hierarchy coordination and the scalability is not altered using the backpropagation approach. The DL-based privacy preservation in IoT was developed by Bi et al., [24]. The collected raw data are separated in a private location at the user end. The fitness-associated facts are scrutinized on fragile security component at the cloud end using a convolution neural network (CNN).

Bordoloi et al., [25] reviewed the current development of ML, DL methods happening in the implementation of healthcare IoT to develop the superiority in the service. The Cipher text policy characteristic-centered encryption structure for smart health care is proposed by Zhang et al., [26]. This privacy-aware smart health access system is provided with a partially hidden approach. This encrypts the smart health data, access policy attributes were hidden and the susceptible data are handled with attribute values. Park et al, [27] proposed an authentication protocol that is vulnerable to capturing attacks by intruders and the plain text that is stored using the key from the user ID and password. It failed to obtain forward secrecy. Uncertainty on the server-based key is identified, then it is easy to compute the session key as the hash value. Shreya et al., [28] developed shared confirmation key contract-based practice is used amongst the medical server, IoT gateway, and user. It accumulates data from medicinal-sensors which are delivered by health care professionals. This procedure implements identical encryption and decryption, XOR, and hashing operations and is vulnerable to password-guessing attacks.

Bahache et al., [29] surveyed the authentication schemes for healthcare applications using wireless medical sensor networks. It classifies the authentication schemes with their architecture with its security and its performance. Jan et al., [30] proposed a wireless medical sensor network-based authentication scheme for the Internet of Medical Things. This paper utilized a cryptographic based relation with public-private key pair on the safety that is serious and reliable. Even though more researchers are developing various lightweight cryptographic approaches to ensure patient security, adaptability, fragility, and security is still an issue due to technological advancement.

3. Proposed System Model and Methods

The patient's private medical data are uploaded to the hospital's centralized location. Then the Machine learning approaches use these data to extract the patterns for real-time monitoring. While this private patient data is visible to the users of the industry then the insider and outsiders hacked the data. Through the Figure 1, this issue, illustrates proposed protected healthcare arrangement that applies DL based privacy preservation model to maintain the secrecy and safety of the patient healthcare data. Unauthorized access to the cloud system is eliminated by encountering various intermediate attacks. For each data access request, the features are stored to analyze the security issues related to activities. From these extracted features, the data quality is determined and the states with their respective actions are taken to ensure the superiority of the data.

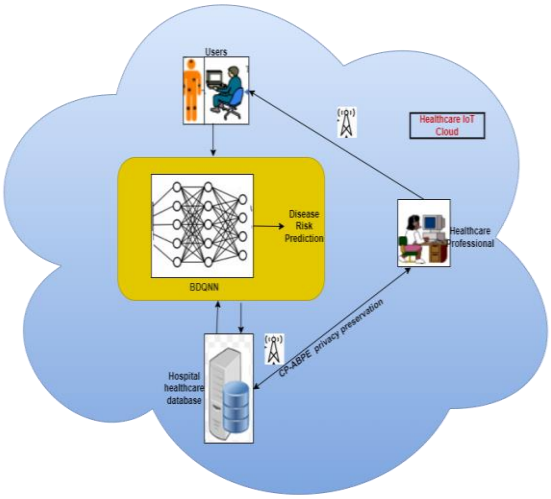

Fig. 1. Overview on proposed system prototype.

Security prototype is shown in Figure 2. It contains a central authority (CA), healthcare professionals, patients who are the users, and a server. The responsibilities of each entity are described as follows:

- Central Authority (CA) – it generates the registration parameters.
- Server - the hospital transfers the medical data of the patient to the server for storage and processing
- User – they are the patients who enquire with the doctors about their medical illnesses.
- The user and health care professionals (HP) interact with the server to provide a clear clinical pathway to the user. Between the hospital and the user, there are multiple interactions permitted which reduces the local communication and computational overhead. The n number of medical data about the patient such as name, age, gender, medication, expenses, and the appointment

time is shared and protected using the authentication system.

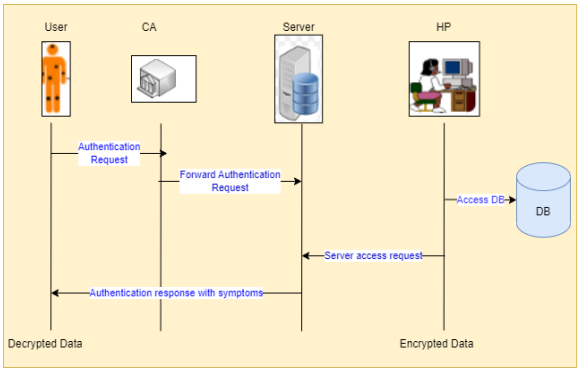

Fig. 2. The proposed security model for data transmission

3.1. Bayesian optimized Deep Q Neural network (BDQNN) based data transmission

DQNN has been utilized here to classify the patient state during the data transmission and further it is optimized with the Bayesian model to ensure the efficiency of the detection of the patient state. Deep Q network [31] is the deep reinforcement learning model based on the optimum value of the Q function gotten from the Deep neural network called Convolution neural network. The neural network comprises of input-module, hidden module, and output stage. The input layer signifies state of the input data, and the output stage exemplifies necessary actions to be taken over the communication channels. The architecture of DQNN is shown in Figure 3.

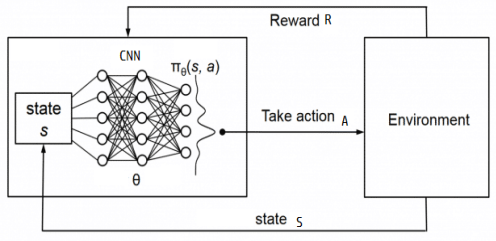

Fig. 3. Deep Q neural network architecture

The hidden layers are comprised of various layers. The number of neurons is computed using Eqn (1)

$$n(h)\sqrt{n(i)+n(o)}+r \quad (1)$$

Where n(h), n(i) and n(o) are the numbers of hidden, input, and output layers respectively, r is the constant in the range [0,10]. The weight (θ) of input and hidden layers and its error is computed using Eqn (2)

$$\delta_t^{DQN} = X_t^{DQN} - Q(S_t, A_t; \theta_t^{DQN}) \quad (2)$$

$$X_t^{DQN} = R_{t+1} + \gamma \quad (3)$$

The weight is updated recursively as in Eqn (4)

$$\theta_{t+1} \leftarrow \theta_t - \alpha\left(\frac{\partial\left(\delta_t^{DQN}\left(\theta_t^Q\right)\right)^2}{\delta_t^Q}\right. \quad (4)$$

In DQNN, the learning rate is fixed based on the target network and experience delay. The Target network is a kind of Q network except for the weight θ is updated with the learning function [32]. In experience delay, the state and its actions along with its rewards are not directly updated where it is stored in replay memory. For training, the data samples are collected from memory. These two learning approaches stabilize the DQNN which reduces the actual and target Q values. The weight of the network is updated using Bayesian optimization. The DQNN is comprised of hyper-parameters like number of hidden modules, activation functions, count of neurons, number of convolution layers in addition to number of iterations, and so on. The tuning of parameters is also a time-consuming process. To reduce the overhead of parameter tuning and weight updation, Bayesian optimization has been utilized. Bayesian optimization reduces the hyperparameters to reduce the loss and computation complexity. It consists of two-step includes initialization and loop update.

(i) Initialization: the loss function is optimized with the Gaussian process.

Initialization

Place Gaussian prior on f

Kernel = gp.kernels.Matern()

Model = gp.GaussianProcessRegression (kernel==kernel)

The true value of f is observed at points n from true loss and set n=m

($y_i = cross\_val\_loss(x_i)$ for i= 1,…m

(ii) Loop update. The posterior is updated with a new sampling point through the acquisition function. The steps for loop update are as follows:

While (n<=N) do

- The posterior probability is updated using all the samples as (model.fit(y_i, x_i))
- Acquisition function maximize x' is identified over the parameter calculated from posterior distribution. In this work, expected improvement acquisition function is used.
- Observe $y' = f(x')$
- $y_n = [y_n, y'], x_n = [x_n, x']$
- $n = n + 1$

End while

3.2. Privacy preservation using Ciphertext-Attribute based policy encryption (CP-ABPE)

The key generation process consists of three processes:

Step 1: the cipher text- quality-centered encryption algorithm may be deployed in obtaining parameters such as master key (mk) and public key (pk).

Step 2: Functional encryption algorithm is utilized to create functional master key (fmk) as well as functional public key (fpk).

s: Key generation algorithm has been utilized to create functional secret key (fsk) which takes F(i) function as input and produces sk[F(i)]as output where i=1,2,3,…n. F(i) has been described in Eqn (5)

$$Fi(S)s_i(KeyGenearation(mk,S))$$
(5)

Where $s_i(s)$ is a function that produces the share (n,k) secret sharing. Once the setup completed, the data users and the ith CA receives the pk_F and $sk[Fi]$ sent by the owner of the data over the secure network respectively.

3.2.1. Sub keys generation

Before the encryption and decryption, the subkeys are created with the help of the following steps. The array of subkeys is pre-computed as B which contains 18 to 32 bits of sub keys.

Input: Plain text

Output: Subkeys

Step 1: Strings (x)=B1,B2,B3,..Bn

Step 2: if

Step 3: A=B1(XOR)B2 (n=B1 and n+1>B1)

Step 4: B=B2 (XOR) B3 (B2=n and B2<n+1)

Step 5: C=B3 (XOR) B4 (n=B1 and n+1>B1)

Step 6: N=Bn (XOR) Bn (B1=n and B1>n+1)

Step 7: end if

Step 8: k1= (A mod E) y*z*

Step 9: k2= (B mod F) x*z*

Step 10: k3= (C mod G) y*x*

Step 11: end

3.2.2. Encryption

The parameter A is assigned with the positive integer where $A \neq g * 257$ and g ranges from 1 to n. R is an array which takes values from 0 to 255 with 256 unique integers. A new array G is created based on A and R which follows linear mapping [33] as in Eqn (6)

$$G(i) = mod\big((A * (R(i) + 1)\big), 257), i \in (1{,}256) \quad (6)$$

Where R(i) takes values from [0,255] and A satisfies $A \neq g * 257$ and g takes integer greater than 0. The function G(i) gets non-zero results then it is transformed into 2-dimensional matrix Gb which is the initial S box. The tent logistic map is repeated for L times to generate the chaotic series. The first (L-256) elements are discarded from actual series and the new chaotic series are generated with the length of 256 for X [18].

3.2.3. Communication with the patients

Based on the node and logic distance as in Eqn (7) [18], a unique ID has been generated for each hospital.

$$d_i\big(H_i, H_j\big) = \frac{\sum_{s,d\in\{H_i\cup H_j - H_i\cap H_j\}} (x_{sd}^{H_i} + x_{sd}^{H_j})}{\sum_{s,d\in H_i\cup H_j} (x_{sd}^{H_i} + x_{sd}^{H_j})}$$
(7)

Where H is the node with ID of Hi(id) and Hj(id) respectively, s is the source and d is the destination. The data privacy is secured using the hospital two nodes randomized approach using Eqn (8)

$$H_r[(a_0) \in S]\ exp\ exp\ (C)\ .H_r[(a') \in O) \quad (8)$$

Where a and a_0 are the adjacent data records and O is the output of received data, C is the total transmission cost and $a \in S$ obtains the data privacy. Using the public and private secret keys pk and sk, encryption is provided for every data in the hospital. Every transaction is estimated as MAE given as in Eqn (9)

$$MAE(T_i) = \frac{1}{n}\sum_{i=1}^{n} \quad |y_i - f(x_i)| \quad (9)$$

Where, T is the training model, n represents count of users, x gives communication cost and y are output respectively. The security risk of sharing the patient personnel data is overcome by transmitting the data to the valid requesters and preserving the holder data privacy.

4. Experimental Results and Discussions

The efficacy of the projected DL based privacy preservation system is analyzed established on the data-accuracy, sensitivity in data, data-specification, data-precision, F1-score, communication overhead, encryption, and decryption time with the selected parameters. The proposed DL with Ciphertext-attribute based policy encryption (CP-ABPE) authentication system ((AS) [BDQNN-AS] is compared with three existing approaches such as mutual authentication protocol (MAP) [14], secure biometric based user authentication scheme (SBUAS) [15], privacy preserving disease prediction (PPDP) [16] and forward privacy preserving model (FPPM) [17].

4.1. DL model performance analysis

Accuracy denotes the ability to predict the overall prediction by the proposed model constructed on four factors such as True positive (TP) and True Negative (TN)

which indicates ability on prediction of presence and absence of an attack. False positive (FP) and false negative (FN) denote untruthful prediction of trained model. The mathematical expression is as in Eqn (10)

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

The sensitivity or recall will detect true positives in the model which is major factor to identify the actual patients with heart disease. It is computed using the Eqn (11)

$$Sensitivity = \frac{TP}{TP+FP} \quad (11)$$

The specificity is the ratio between actual negatives predicted as negative. It is also known ias true negative rate as shown in Eqn (11)

$$Specificity = \frac{TP}{TP+FN} \quad (12)$$

Data-Precision is relation between true positive and altogether the positives denoted in Eqn (13)

$$Precision = \frac{TP}{TP+FP} \quad (13)$$

The accuracy comparison of existing and proposed model is illustrated in Figure 4. The x axis symbolizes the count of epochs used for examination and y axis denotes the secured accuracy. This comparison results shows that the conventional approaches such as MAP secured the accuracy of 94.5%, SBUAS secured 92.8%, PPDP secured 92.9% and FPPM obtained 93.9%. The proposed BDQNN-AS obtained the accuracy of 98.3% which was 3.8% better than MAP, 5.5% better than SBUAS, 5.4% better than PPDA and 4.4% better than FPPM.

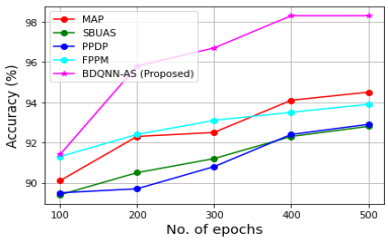

Fig. 3. Accuracy comparison

Using Figure 5 and Figure 6 respectively, Sensitivity and specificity comparison of existing and proposed methodology is showed. The x axis designates the count of epochs used for examination and y axis denotes the obtained sensitivity. This comparison results shows that the conventional approaches such as MAP secured the sensitivity of 81.2%, SBUAS secured 84.6%, PPDP secured 83.6% and FPPM obtained 85.9%. The proposed BDQNN-AS obtained the sensitivity of 94.2% which was 13% better than MAP, 9.6% better than SBUAS, 10.6% better than PPDA and 8.3% better than FPPM.

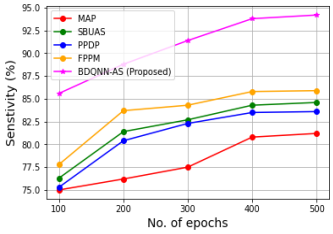

Fig. 4. Sensitivity comparison

The illustration of Figure 6 describes the specificity comparison. The x axis denotes the number of epochs used for examination and y axis denotes the achieved specificity. This comparison results shows that the conventional approaches such as MAP secured the specificity of 91.6%, SBUAS secured 95.6%, PPDP secured 93.5% and FPPM obtained 95.8%. The proposed BDQNN-AS obtained the specificity of 96.9% which was 5.3% better than MAP, 1.3% better than SBUAS, 3.4% better than PPDA and 1.1% better than FPPM.

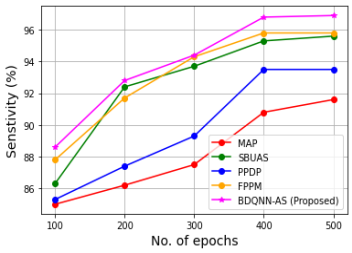

Fig. 5. Specificity comparison

In Figure 7, comparison in terms of precision is shown. The x axis indicates count of epochs used for examination and y axis denotes the obtained precision. This comparison results shows that the conventional approaches such as MAP secured the accuracy of 91.2%, SBUAS secured 89.4%, PPDP secured 89.1% and FPPM obtained 94.2%. The proposed BDQNN-AS obtained the accuracy of 95.9% which was 4.7% better than MAP, 6.5% better than SBUAS, 6.8% improved than PPDA and 1.7% better than FPPM.

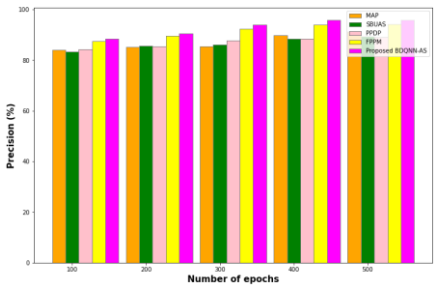

Fig. 6. Precision comparison

4.2. Security analysis of proposed model

The proposed model efficiency for security analysis is evaluated in terms of communication overhead (CO), Encryption time (ET) and Decryption time (DT). Communication overhead are ratio of total count of data-

packets communicated from source node x to endpoint node y within a less time using Eqn (14)

$$CO = \sum_{0}^{No.of\ packets} \quad x \rightarrow y \tag{14}$$

Encryption time (ET) in ms is the time consumed by the approach to convert the plain text P to cipher text C using the keys which is computed using Eqn (15)

$$ET = Time(P \rightarrow C) \tag{15}$$

Decryption time (ET) in ms is the time consumed by the approach to convert cipher text C to plain text P using the keys which are computed using Eqn (16)

$$DT = Time(C \rightarrow P) \tag{16}$$

Figure 8 illustrates the communication overhead comparison of proposed and existing approaches. The x axis denotes the number of epochs intended for exploration and y axis stand for attained communication overhead on percentages. This comparison results shows that the conventional approaches such as MAP secured the CO of 64.9%, SBUAS secured 64.4%, PPDP secured 63.4% and FPPM obtained 65.3%. The proposed BDQNN-AS obtained the CO of 68.1% which was 3.2% better than MAP, 3.7% better than SBUAS, 4.7% better than PPDA and 2.8% better than FPPM.

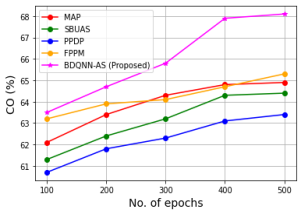

Fig. 7. Communication overhead comparison

Figure 9 and Figure 10 illustrate the comparison of encryption and decryption time in ms, in which the number of epochs are measured as x-y axis's denotes the encryption plus decryption time on milliseconds. When compared, the results of Figure 9 shows that the conventional approaches such as MAP secured the ET of 66.3%, SBUAS secured 65.1%, PPDP secured 66.2% and FPPM obtained 61.3%. The proposed BDQNN-AS obtained an ET of 59.4% which was 6.9% faster than MAP, 5.7% faster than SBUAS, 6.8% faster than PPDA and 1.9% faster than FPPM.

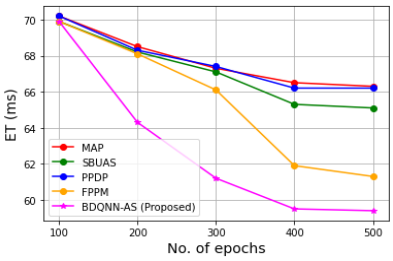

Fig. 8. Encryption time (ms) comparison

The comparison illustration from Figure 10, the decryption time results shows that the conventional approaches such as MAP secured the ET of 67.2%, SBUAS secured 66.3%, PPDP secured 67.4% and FPPM obtained 62.7%. The proposed BDQNN-AS obtained the ET of 60.2% which was 7% faster than MAP, 6.1% faster than SBUAS, 7.2% faster than PPDA and 2.5% faster than FPPM. Hence, all the comparison outcomes prove the effectiveness of projected prototype. In all the analysis, the average result was obtained during the epochs 400 and 500. After that the results did not change. Therefore, the optimal epoch for proposed system is considered as 500 and complete qualified outcomes are shown in Table 1.

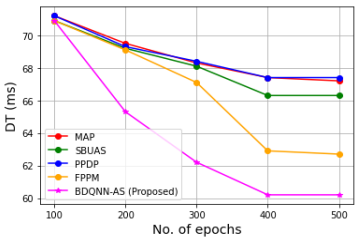

Fig. 9. Decryption time comparison

Table 1. The overall comparison of existing and proposed model performance

Methods	Parameters						
	Accuracy (%)	Sensitivity (%)	Specificity (%)	Precision (%)	CO (%)	ET (ms)	DT (ms)
MAP	94.5	81.2	91.6	91.2	64.9	66.3	67.2
SBUAS	92.8	84.6	95.6	89.4	64.4	65.1	66.3
PPDP	92.9	83.6	93.5	89.1	63.4	66.2	67.4
FPPM	93.9	85.9	95.8	94.2	65.3	61.3	62.7
BDQNN-CPABPE (Pro	**98.3**	**94.2**	**96.9**	**95.9**	**68.1**	**59.4**	**60.2**

pose d)							

5. Conclusion

For the healthcare IoT systems, the safety and secrecy of the patient data is a big challenge. Due to limitation of resources in IoT, the previous security systems are not sufficient, and it is needed to develop a model that enhances the security of the healthcare systems. In order to develop a secure IoT based healthcare system, the DL based privacy preservation model has been proposed in this paper that refuses malicious users through the authentication system and monitors the patient health data securely. The Bayesian optimized Deep Q neural network may be implemented on manipulation of sick-person data's for real time monitoring which will reduce the network traffic. Further, the patient data has been secured while transmission by adopting Ciphertext-attribute based policy encryption (CP-ABPE) authentication system (AS) which has been proposed to encrypt the patient data and decrypted by the authorized users. The sturdiness in addition the efficacy of the proposed model are assessed underneath several environments and its outcomes is investigated with the comparison. The proposed BDQNN-CPABPE model secured an improved accuracy of 98.3% on processing the patient data accurately and obtained reduced encryption and decryption time of 59.4ms and 60.2ms respectively. In future, the cost and time constraints are further reduced with the implementation of larger datasets in fog computing to generalize the proposed model performance. The block chain-based securities models are also incorporated further to ensure the user identify protections.

Funding

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Conflict of interest

The authors declare that they have no conflict of interest.

Author Contributions

All authors read and approved the final manuscript.

Data Availability Statement

Data sharing not applicable to this article, because it's confidential.

Ethical Approval

The article does not contain any studies with Human Participants or animals performed by any of the Authors.

References

[1] Empowering the Health Workforce: Strategies to Make the Most of the Digital Revolution; Technical Report; Organization for Economic Co-Operation and Development (OECD): Paris, France, 2020. Available online: https://www.oecd.org/publications/ empowering-the-health-workforce-to-make-the-most-of-the-digital-revolution-37ff0eaa-en.htm (accessed on 6 July 2022).

[2] Hallberg, D., & Salimi, N. (2020). Qualitative and Quantitative Analysis of Definitions of e-Health and m-Health. Healthcare informatics research, 26(2), 119-128.

[3] Wan, H., Zhuang, L., Pan, Y., Gao, F., Tu, J., Zhang, B., & Wang, P. (2020). Biomedical sensors. In Biomedical Information Technology (pp. 51-79). Academic Press.

[4] Angelov, G. V., Nikolakov, D. P., Ruskova, I. N., Gieva, E. E., & Spasova, M. L. (2019). Healthcare sensing and monitoring. In Enhanced Living Environments: Algorithms, Architectures, Platforms, and Systems (pp. 226-262). Cham: Springer International Publishing.

[5] Kathamuthu, N. D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M., & Gandomi, A. H. (2022). Deep Q-learning-based neural network with privacy preservation method for secure data transmission in internet of things (IoT) healthcare application. Electronics, 11(1), 157.

[6] Ramos, J. L. H., Bernabé, J. B., & Skarmeta, A. F. (2014, July). Towards privacy-preserving data sharing in smart environments. In 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 334-339). IEEE.

[7] Guo, X., Duan, X., Gao, H., Huang, A., & Jiao, B. (2013). An ecg monitoring and alarming system based on android smart phone. Communications and Network, 5(03), 584-589.

[8] Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. In The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care (pp. 105-134). Cham: Springer International Publishing.

[9] Mousavi, S. K., Ghaffari, A., Besharat, S., &

Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks, 27, 1515-1555.

[10] Rahim, R., Murugan, S., Mostafa, R. R., Dubey, A. K., Regin, R., Kulkarni, V., & Dhanalakshmi, K. S. (2020). Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords. Webology, 17(2).

[11] Tang, J., Liu, A., Zhao, M., & Wang, T. (2018). An aggregate signature based trust routing for data gathering in sensor networks. Security and Communication Networks, 2018.

[12] Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. Ieee Access, 6, 52843-52856.

[13] Otoum, S., Kantarci, B., & Mouftah, H. T. (2019). On the feasibility of deep learning in sensor network intrusion detection. IEEE Networking Letters, 1(2), 68-71.

[14] El-Meniawy, N., Rizk, M. R., Ahmed, M. A., & Saleh, M. (2022). An Authentication Protocol for the Medical Internet of Things. Symmetry, 14(7), 1483.

[15] Deebak, B. D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2019). An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. IEEE Access, 7, 135632-135649.

[16] Zhang, C., Zhu, L., Xu, C., & Lu, R. (2018). PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system. Future Generation Computer Systems, 79, 16-25.

[17] Wang, K., Chen, C. M., Tie, Z., Shojafar, M., Kumar, S., & Kumari, S. (2021). Forward privacy preservation in IoT-enabled healthcare systems. IEEE transactions on industrial informatics, 18(3), 1991-1999.

[18] Kathamuthu, N. D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M., & Gandomi, A. H. (2022). Deep Q-learning-based neural network with privacy preservation method for secure data transmission in internet of things (IoT) healthcare application. Electronics, 11(1), 157.

[19] Ahamad, D., Hameed, S. A., & Akhtar, M. (2022). A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. Journal of King Saud University-Computer and Information Sciences, 34(6), 2343-2358.

[20] Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C., & Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing, 1-21.

[21] Hui, H., Zhou, C., Xu, S., & Lin, F. (2020). A novel secure data transmission scheme in industrial internet of things. China Communications, 17(1), 73-88.

[22] Abirami, P., & Bhanu, S. V. (2020). Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment. Soft Computing, 24, 18927-18936.

[23] Zhang, L., Shi, Y., Chang, Y. C., & Lin, C. T. (2020). Hierarchical fuzzy neural networks with privacy preservation for heterogeneous big data. IEEE Transactions on Fuzzy Systems, 29(1), 46-58.

[24] Bi, H., Liu, J., & Kato, N. (2021). Deep learning-based privacy preservation and data analytics for IoT enabled healthcare. IEEE Transactions on Industrial Informatics, 18(7), 4798-4807.

[25] Bordoloi, D., Singh, V., Sanober, S., Buhari, S. M., Ujjan, J. A., & Boddu, R. (2022). Deep learning in healthcare system for quality of service. Journal of Healthcare Engineering, 2022.

[26] Zhang, Y., Zheng, D., & Deng, R. H. (2018). Security and privacy in smart health: Efficient policy-hiding attribute-based access control. IEEE Internet of Things Journal, 5(3), 2130-2145.

[27] Park, K., Noh, S., Lee, H., Das, A. K., Kim, M., Park, Y., & Wazid, M. (2020). LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things. IEEE Access, 8, 119387-119404.

[28] Shreya, S., Chatterjee, K., & Singh, A. (2022). A smart secure healthcare monitoring system with Internet of Medical Things. Computers and Electrical Engineering, 101, 107969.

[29] Bahache, A. N., Chikouche, N., & Mezrag, F. (2022). Authentication schemes for healthcare applications using wireless medical sensor networks: A survey. SN Computer Science, 3(5), 382.

[30] Jan, S. U., Ali, S., Abbasi, I. A., Mosleh, M. A., Alsanad, A., & Khattak, H. (2021). Secure patient authentication framework in the healthcare system using wireless medical sensor networks. Journal of Healthcare Engineering, 2021.

[31] Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A.,

Veness, J., Bellemare, M. G., ... & Hassabis, D. (2015). Human-level control through deep reinforcement learning. nature, 518(7540), 529-533.

[32] Lillicrap, T. P., Hunt, J. J., Pritzel, A., Heess, N. M. O., Erez, T., Tassa, Y., ... & Wierstra, D. P. (2020). U.S. Patent No. 10,776,692. Washington, DC: U.S. Patent and Trademark Office.

[33] Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2014, November). A novel design of Chaos based S-Boxes using genetic algorithm techniques. In 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA) (pp. 678-684). IEEE.