

Article

Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application

Nirmala Devi Kathamuthu ¹, Annadurai Chinnamuthu ², Nelson Iruthayanathan ², Manikandan Ramachandran ³ and Amir H. Gandomi ^{4,*} 

¹ Department of CSE, Kongu Engineering College, Perundurai, Erode 638060, Tamil Nadu, India; k_nirmal@kongu.ac.in

² Department of ECE, Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, Chennai 603110, Tamil Nadu, India; annaduraic@ssn.edu.in (A.C.); nelson@ssn.edu.in (N.I.)

³ School of Computing, SASTRA Deemed University, Thanjavur 613401, Tamil Nadu, India; srmanimt75@gmail.com

⁴ Data Science Institute, Faculty of Engineering and Information Systems, University of Technology Sydney, Ultimo, Sydney, NSW 2007, Australia

* Correspondence: gandomi@uts.edu.au

Abstract: The healthcare industry is being transformed by the Internet of Things (IoT), as it provides wide connectivity among physicians, medical devices, clinical and nursing staff, and patients to simplify the task of real-time monitoring. As the network is vast and heterogeneous, opportunities and challenges are presented in gathering and sharing information. Focusing on patient information such as health status, medical devices used by such patients must be protected to ensure safety and privacy. Healthcare information is confidentially shared among experts for analyzing healthcare and to provide treatment on time for patients. Cryptographic and biometric systems are widely used, including deep-learning (DL) techniques to authenticate and detect anomalies, and provide security for medical systems. As sensors in the network are energy-restricted devices, security and efficiency must be balanced, which is the most important concept to be considered while deploying a security system based on deep-learning approaches. Hence, in this work, an innovative framework, the deep Q-learning-based neural network with privacy preservation method (DQ-NNPP), was designed to protect data transmission from external threats with less encryption and decryption time. This method is used to process patient data, which reduces network traffic. This process also reduces the cost and error of communication. Comparatively, the proposed model outperformed some standard approaches, such as these secure and anonymous biometric based user authentication scheme (SAB-UAS), MSCryptoNet, and privacy-preserving disease prediction (PPDP). Specifically, the proposed method achieved accuracy of 93.74%, sensitivity of 92%, specificity of 92.1%, communication overhead of 67.08%, 58.72 ms encryption time, and 62.72 ms decryption time.

Keywords: healthcare; deep learning; privacy; Internet of Things (IoT); Q-learning; data transmission



Citation: Kathamuthu, N.D.; Chinnamuthu, A.; Iruthayanathan, N.; Ramachandran, M.; Gandomi, A.H. Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application. *Electronics* **2022**, *11*, 157. <https://doi.org/10.3390/electronics11010157>

Academic Editor: Valeri Mladenov

Received: 30 November 2021

Accepted: 29 December 2021

Published: 4 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Things (IoT) utilizes IP-based communication for connecting the Internet with sensors and a multitude of devices. For instance, healthcare sectors with the IoT can achieve remote monitoring, early diagnosis, treatment, and prevention [1]. Moreover, objects or people was furnished with sensors, such as radio-frequency identification (RFID) tags, and actuators in IoT to monitor the status. The RFIDs tags or personal medical devices of patients can be read, located, recognized, and controlled using IoT applications [2]. Several smart applications and services can overcome the challenges faced by individuals and the healthcare industry [3] by using the dynamic abilities of the IoT to connect objects

to objects, devices to machines, patients to machines, patients to doctors, doctors to machines, mobiles to humans, sensors to mobiles, and tags to readers. Machines, humans, dynamic systems, and smart devices are intellectually connected to ensure the efficiency of a healthcare system [4]. In general, the IoT structure comprises 3 layers, namely, the network, perception, and application layers. The perception layer is responsible for collecting healthcare data using several devices [5]. The network layer consists of wired, wireless, and middleware systems, and progresses and transfers the input from the perception layer. When designed efficiently, transport protocols can improve the efficiency of data transmission, decrease the consumption of energy, and ensure privacy and security [6]. The application layer combines the sources of medical data and offers medical services that satisfy the needs of the user on the basis of the current situation and demand. Privacy and security information related to patients is the most essential concept in an IoT-based environment [7]. Data security can be achieved by securely storing and transferring data, ensuring integrity, authenticity, and validity. Data privacy is achieved when data are accessed only by authorized individuals [8]. On the basis of demands, purposes, and needs, protection strategies can be reasonably developed. Although widely used IoT devices can help in improving the health of patients, securing and protecting human information must be achieved at the same time. As attacks have increased on next-generation systems, IoT devices are susceptible to both unknown and known attacks [9]. Data that flow from the IoT domain to the cloud and visualization domains are altered at several points in the cloud hierarchy. Conventional systems based on signature or machine-learning approaches are not capable of dealing with the current situation due to the frequent occurrence of unknown attacks. Deep neural networks (DNNs) can detect a virtualized communication network failure by recognizing the normal data flow and reconstructing it for higher accuracy [10]. However, the major challenge faced with these models is that more training time is required for complex DNNs in the core clouds compared to existing traditional methods. Hence, it is necessary to develop innovative approaches that reduce the training time without compromising detection accuracy.

The contribution of this work is as follows:

- Constructing a systematic framework using the deep Q-learning method for processing patient data, which further reduces traffic in a network.
- Adopting ciphertext-policy attribute-based privacy preservation (CPABPP) for generating both a public key (PK) and a master key (MK).

This paper is organized as follows. Section 1 describes the background of the Internet of Things (IoT) in healthcare, security and privacy issues, and the role of deep learning in the security field. In Section 2, the literature of reported privacy preservation methods in healthcare IoT is reviewed. Section 3 explains the proposed privacy preservation method by constructing a system model. In Section 4, experimental analysis is given with graphs by comparing three standard methods. Lastly, Section 5 presents the conclusion and future research directions.

2. Related Works

The authors in [11] utilized advanced artificial-intelligence approaches to develop a model that preserves data privacy in the cloud. This model involves two main stages: the sanitization and restoration of data. The process of sanitization is based on generating an optimal key using the hybrid metaheuristic Jaya-based shark smell optimization (J-SSO) method. A multi-objective function was derived having parameters such as hiding ratio, degree of modification, and ratio of information preservation to generate the optimal key. A secure and anonymous biometric-based user authentication scheme (SAB-UAS) was developed in [12] that securely ensures communication in the healthcare industry. Results proved that an imposter does not act as a genuine user for accessing or cancelling a handheld smart card. A forward privacy preservation scheme was presented in [13] for healthcare systems based on IoT. This scheme involved trapdoor permutation for changing the status counter, making it hard for an adversary to determine the valid status counter of the record with only the client public key; this was developed in [14]. A modified deep residual network

was designed in [15], in which new smooth pooling layers were defined to leverage the performance of the model. The researchers also suggested a method to recognize human activities in an IoT cloud environment, thereby enabling users to create situations on the basis of their actions at home. An architecture of function as a service (FaaS) was involved to solve the problem of scalability, whereby every function was executed in a distinct container. The privacy-preserving disease prediction (PPDP) method was developed in [16] to efficiently encrypt and store patients' medical data in the cloud server for further processing. Prediction models were trained with the single-layer perceptron learning method. An optimal deep-learning-based secure blockchain (ODLSB)-enabled intelligent IoT model for healthcare diagnosis was presented in [17]. This model involved 3 main processes: secured transaction, the encryption of hash values, and medical diagnosis. From the obtained results, many features were formed with higher sensitivity (92.75%), accuracy (93.68%), and specificity (91.42%). Varying-structure fractional-order chaotic-system synchronization with varying order was presented in [18]. The theory of Lyapunov stability was utilized to establish synchronization between the response system and fractional-order drive system. The process of encrypting and decrypting major data signals is executed by utilizing the principle of n -shift encryption. The simulation results showed the effectiveness of the theoretical approach. A secure Fabric block chain-established data transmission approach in industrial IoT was explained in [19]. This approach utilizes the blockchain-based dynamic mechanism of secret sharing. This technique improves the rate of transmission and rate of packet receiving by 12% and 13%, respectively. Furthermore, this approach can achieve a better management of sharing and decentralization. A distributed secure outsourcing scheme was improved in [20] by utilizing a crypto-deep neural network. This technique possesses a web server, cloud server, cloud agent, and data center. In-personalization attacks are handled by crypto-deep neural network cloud security (CDNNCS). A nearly 10% reduction in packet loss was obtained from the results of CDNNCS, and a 5% increase in response time compared to the existing approach. A privacy-preserving hierarchical fuzzy neural network was trained in [21] with a two-stage optimization algorithm, and the hierarchy's low-level parameters were learnt with a model depending on the familiar method of alternating-direction multipliers, which does not expose local data to other agents. Higher levels of hierarchy coordination are processed by another method of optimization that is quickly converged. The overall procedure's scalability and speed are not altered by problems of gradient vanishing, such as backpropagation models. The efficiency of the proposed technique was demonstrated by classification and regression approaches based on simulation. For IoT-enabled healthcare, the deep-learning-based preservation of privacy and a system of data analytics was presented in [22]. At the user end, raw data are gathered, and the private information of users is separated in the zone of privacy isolation. At the cloud end, health-associated information analysis, with no private data of users and fragile security components, is conducted depending on the convolutional neural network (CNN). Efficiency and robustness were proven by experimental analysis. A novel Q-learning-based transmission process for scheduling was developed in [23], utilizing deep learning for the IoT for solving the issue for achieving the suitable plan for the transmission of packets with various buffers by several channels for the maximization of the throughput of system. A Markov decision process-dependent technique is computed for describing the system's transformation of state. This method produces enhanced packet transmission with lower power consumption and packet loss. An intelligent trust cloud management approach was presented in [24]. A trust cloud update technique was developed for the adaptive and intelligent management of the trust approach belonging to an open wireless medium. Results demonstrated that this approach can efficiently introduce uncertainty in trust problems, and accuracy for the detection of malicious devices was improved. A cascade-learning-embedded vision inspection method of rail fasteners based on a deep convolutional neural network (DCNN) was presented in [25]. A convolutional neural network (CNN) is used for faulty fastener detection. Extensive experiments were conducted to demonstrate this method's performance. Experimental results showed that this method

realized average precision and recall of 95.38% and 98.62%, respectively, on a fast detecting mechanism, which is highly more efficient than the physical operation.

Although the review of related works reveals that much focus has been directed to developing security and privacy models for the healthcare sector, improved security and privacy are yet to be achieved. Conversely, several privacy systems are not suitable for providing effective security measures. To overcome these problems, a deep Q-learning-based neural network was employed with the privacy preservation method (DQ-NNPP) in this work, which is discussed below.

3. System Model

Private patient data, which are essential for hospital applications, are uploaded in centralized locations. Then, machine-learning techniques utilize these data to extract unique patterns for developing models. When such private data become visible to the members of the company or if the company dataset is hacked, insider and outsider threats occur, respectively.

As shown in Figure 1, the constructed model applies neural-network techniques for maintaining the security and privacy of healthcare information. Here, several intermediate attacks are encountered by the system; hence, unauthorized access to the cloud storage must be eliminated. Once user data are obtained, for every request, features are extracted and stored to analyze malware activities and issues related to security and privacy. From these features, the quality value of data can be determined with the use of feature states, and their corresponding actions help to determine the data quality.

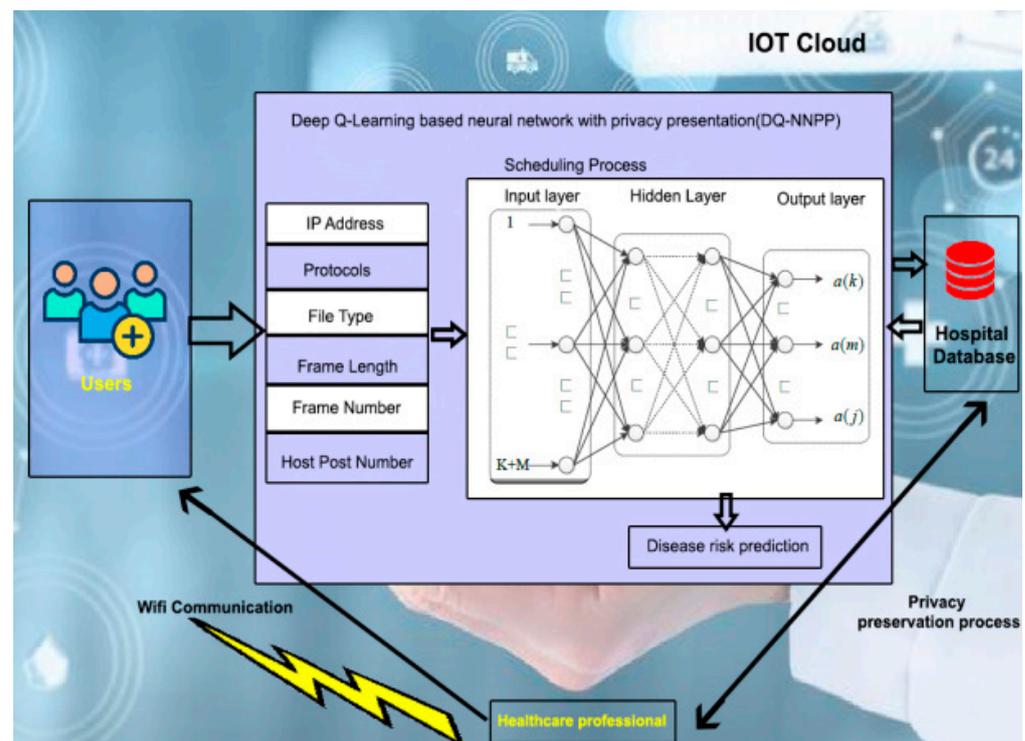


Figure 1. System architecture of privacy preservation method in IoT healthcare infrastructure.

3.1. Deep Q-Learning-Based Scheduling and Data Transmission

Input = $[a_1 \text{ to } f_1, a_2 \text{ to } f_2 \dots a_n \text{ to } f_n]$ signifies the system state's information, and $a + b$ indicates the neuron number in the layer. The output layer representing the information of the selection action is illustrated in Figure 2, which contains the channel (m) in communica-

tion mode j and buffer k with $a + b + J$ neurons. The hidden layer is composed of several layers, and the number of neurons is estimated using Equations (1) and (2):

$$N(h) = \sqrt{n(i) + n(o)} + \text{Con.} \quad (1)$$

$$W = \{(w_{ij}) \in (n * m)\} \quad (2)$$

where $n(i)$, $n(o)$, and $N(h)$ are the numbers of the input, output, and hidden layers, respectively; Con indicates a constant limited in Con [1,10]; and w_{ij} represents the weight between the i -th visible and j -th hidden cells. For the process of encoding and decoding, the logistic sigmoid function is used as a transfer function. The cost function is defined by $L(x)$ [23], as shown in Equation (3):

$$L(x) = \arg \min \sum_{i=1}^n \frac{x_i - f_i}{2} + J(m) \quad (3)$$

where $J(m)$ is the weight decay that reduces the weight, thereby preventing overfitting during training. To update the weight and bias vector, the rules in Equations (4) and (5) are used:

$$W(k + 1) = W(k) - \beta \quad (4)$$

$$B(k + 1) = b(k) - \beta \quad (5)$$

where the learning rate is denoted by β . The residual error's backpropagation is δ , which is given in Equations (6) and (7):

$$\Delta_{im} = \Delta_{im} + 1 \times W_{ij} \times f_m \quad (6)$$

$$A = \{b_i \in \mathbb{R}^n\} \quad (7)$$

where b_j is the bias threshold of the j -th visible cell. Consider that the visible and hidden layers follow Bernoulli distribution; then, the order of (v, h) is represented as shown in Equation (8):

$$E(v, h | \theta) = -\sum n_i = 1 a_i v_i - \sum m_j = 1 b_j h_j - \sum n_i = 1 \sum n_i = 1 v_i w_{ij} h_j \quad (8)$$

where $\theta = \{W_{ij}, a_i, b_j\}$, and the energy function indicates the estimated energy in every node of the visible and hidden layers.

System Model for Security

Here, the security for medical record datasets, and preserving the privacy of patients and hospitals is achieved. This model contains a trusted authority (TA), hospitals with healthcare professionals, patients (user), and a server, as shown in Figure 3.

The roles of each entity in the system model are described below:

- TA generates the parameters and deals with registration.
- Hospitals supply patients' medical information to the servers.
- The user queries the doctors with the source and destination stage.
- Interaction between servers generates a portion of the clinical pathway, which in turn is returned to the user. Multiple interactions are allowed to occur with other interactions instead of between the hospital and user, thereby effectively reducing the local communication overhead and computational cost. In this model, the data ($k = 1, 2, 3, \dots, m$) of medical datasets include details of the patients, such as name, age, gender, expenses, other indices, medication, and the time of appointments. These details are shared and protected by the ciphertext-policy attribute-based privacy preservation approach. On the basis of these privacy policies, the server creates an integrated directional connected network.

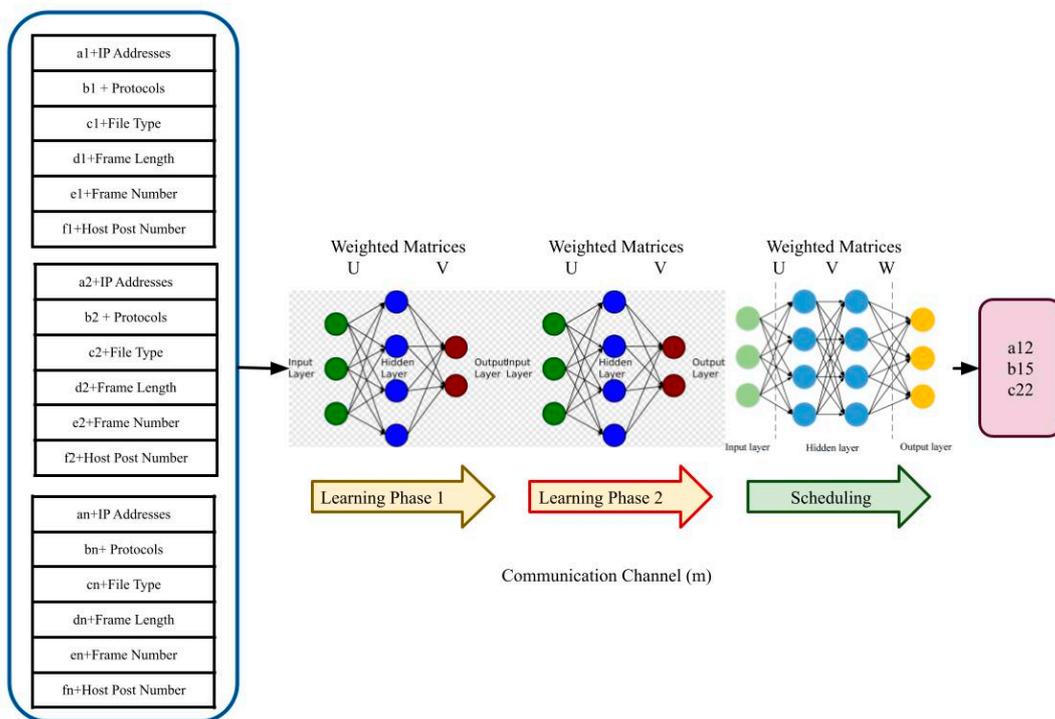


Figure 2. Data scheduling from patients using deep Q-learning.

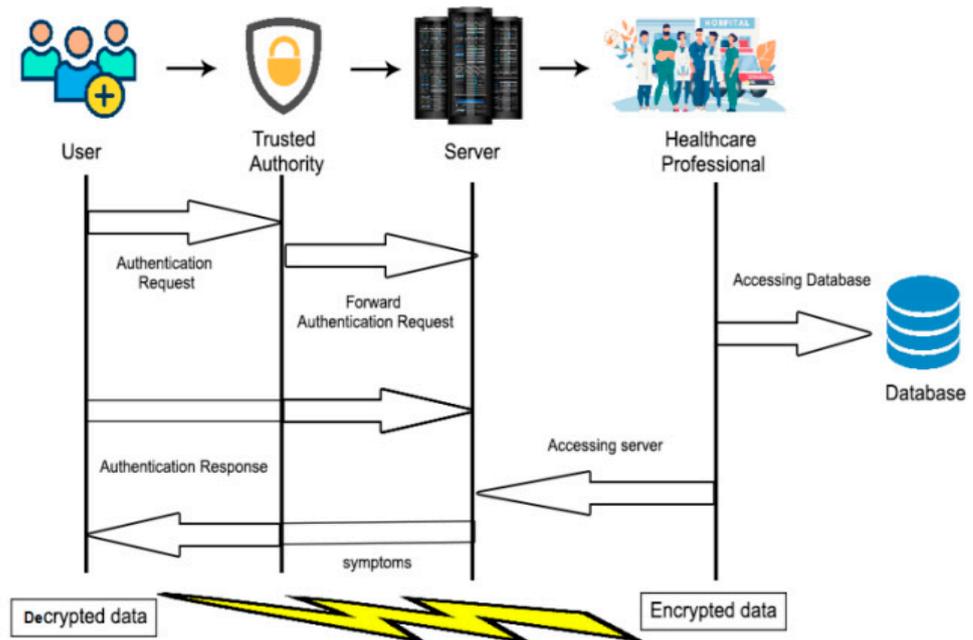


Figure 3. System model for securable data transmission to the healthcare provider.

3.2. Key Generation on Ciphertext-Policy Attribute-Based Privacy Preservation (CPABPP)

The data owner executes the setup algorithm, which comprises three steps.

Step 1: the CP-ABE setup algorithm is applied, obtaining a few security parameters as input; a public key (PK) and a master key (MK) are generated.

Step 2: the functional encryption setup algorithm is applied, which uses a few security measures as inputs to produce a functional master key (MKF) and functional public key (PKF).

Step 3: The key-generating algorithm $KeyGen(MK, S)$ of functional encryption is applied, where function $f(i)$ is taken as the input to generate a functional secret key $SK[f(i)]$ as

the output, here $i = 1, 2, \dots, n$. $f(i)$ is described as $f_i(S) = ss_i(\text{KeyGen}(\text{MK}, S))$, where $ss_i(s)$ is a function that produces the share as (n, k) secret sharing is applied on secrets. Once the setup algorithm is executed, data users and the i -th authority receive PK_F and $SK [f_i]$ sent by the data owner over the secure channel, respectively. In this process, a large number of subkeys are used, which are precomputed before the process of decryption or encryption. The P-array contains 18 to 32 bit subkeys: P_1, P_2, \dots, P_{18} .

Algorithm 1 for generating subkeys:

Algorithm 1 Algorithm for generating subkeys

```

1: Input—plain text
2: Output—subkeys
3: Strings(x) = P1, P2, P3 ... Pn
4: if
5: A = P1(XOR) P2
6: (n = P1; n + 1 > P1)
7: B = P2(XOR) P3
8: (P2 = n; P2 < n + 1)
9: C = P3(XOR) P4
10: (n = P1; n + 1 > P1)
11: N = Pn(XOR) Pn
12: (P1 = n; P1 < n + 1)
13: end if
14: Y*Z*(A mod E) = K1
15: X*Z*(B mod F) = K2
16: Y*X*(C mod G) = K3
17:  $\alpha^2 (Y*Z*(A \text{ mod } E)) = \beta K1$ 
18:  $\alpha^2 (X*Z*(B \text{ mod } F)) = \beta K2$ 
19:  $\alpha^2 (Y*X*(C \text{ mod } G)) = \beta K3$ 
20: end

```

Encryption Process

Parameter A is assigned a positive integer value, such that $A \neq k \times 257$, where k ranges from 1 to n . Consider an array T taking values from 0 to 255, and thus a total of 256 unique integers. A new array R is obtained on the basis of A and T that follows linear mapping [26] as given in Equation (9):

$$R(i) = \text{mod}((A \times (T(i) + 1)), 257) \tag{9}$$

where i ranges from 1 to 256. $T(i)$ takes values from 0 to 255; positive integer A satisfies $A \neq k \times 257$, and k takes up an integer greater than 0. $(A/257)$ and $(T(i) + 1)/257$ yield non integer values, such that they are not exactly divisible by 257. Thus, $\text{mod}((A \times (T(i) + 1)), 257)$ is nonzero. Consider $R(i) \leftarrow R(i) - 1$; then, $R(i)$ ranges from 0 to 255, where i is 1 to 256. The 1D array $R = \{R(i)\}$ is then transformed into a 2D matrix R_b , which is the initial S-box. The tent-logistic map is then repeated L times to generate a chaotic series with length L . The sensitivity of the chaotic series is improved, as the first $(L-256)$ elements are discarded from the actual chaotic series, thereby obtaining a new chaotic series with length 256 denoted as X . By sorting X , $J = \{J(1), J(2), \dots, J(256)\}$, an index array, is obtained. As the chaotic series is nonperiodic and ergodic, it certainly gives $J(i) \neq J(j)$, provided that $i \neq j$.

C. Communication with diagnosed patients

A unique ID is generated by each hospital on the basis of logic and node distance, as shown in Equation (10):

$$d_i(H_i, H_j) = \frac{\sum_{p,q \in \{H_i \cup H_j - H_i \cap H_j\}} (x_{pq}^{H_i} + x_{pq}^{H_j})}{\sum_{p,q \in H_i \cup H_j} (x_{pq}^{H_i} + x_{pq}^{H_j})} \tag{10}$$

where H_i and H_j are nodes with IDs of $H_i(\text{id})$ and $H_j(\text{id})$, respectively; p is the source; and q is the destination. Data privacy is secured in a decentralized way [27] using a randomized approach for two nodes of hospitals, as shown in Equation (11):

$$\text{Hr}[(R_0) \in S] \leq \exp(\epsilon) \cdot \text{Hr}[(R') \in O] \quad (11)$$

where R and R_0 represent adjacent data records, and O indicates the set of data received as output. $R \in S$ achieves data privacy, but for several hospitals, Laplace is put into local training model m_i , as shown in Equation (12):

$$\vec{m}_1 = m_i + \text{Laplace}(s/\epsilon) \quad (12)$$

where s stands for sensitivity; and ϵ indicates the total cost for transmission. For the preservation of data privacy in hospitals, encryption is provided on every data by public and private keys (PK_i, SK_i). MAE estimates every transaction and broadcasts H_j via MAE (m_i) and MAE (H_j). Every record of the approved transaction is maintained in the distributed ledger. MAE is given in Equation (13):

$$\text{MAE}(m_i) = \frac{1}{n} \sum_{i=1}^n |y_i - f(x_i)| \quad (13)$$

where n indicates the total number of users; and x_i indicate the communication and transaction cost, respectively. Sharing personal data is a risk for data providers due to some specific security attacks. This can be overcome by simply transmitting data to the user with valid details to the requester, and preserving the data privacy of the holders. Rather than sharing actual data, learned models alone can be exchanged by the provided data, such as hospitals with the requester.

4. Performance Analysis

For analysis, accuracy, sensitivity, specificity, communication overhead, time of encryption, and time of decryption were selected as the parameters. The proposed deep Q-learning-based neural network with the privacy preservation method (DQ-NNPP) was compared with three standard methods, namely, the secure and anonymous biometric-based user authentication scheme (SAB-UAS), MSCryptoNet, and privacy-preserving disease prediction (PPDP) on the basis of these parameters.

Accuracy presents the ability of the overall prediction produced in this approach. True-negative (TN) and true-positive (TP) indicate the capability of predicting the absence or presence of an attack. False-negative (FN) and false-positive (FP) reflect false predictions by the used model. The formula for accuracy is given in Equation (14):

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (14)$$

Figure 4 illustrates the comparison of accuracy between the existing SAB-UAS, MSCryptoNet, PPDP methods, and the proposed DQ-NNPP method, where the X-axis displays the number of epochs utilized for the examination, and the Y-axis represents the obtained accuracy values in percentages. When compared, the SAB-UAS, MSCryptoNet, and PPDP methods achieved accuracy of 92.02%, 94.3%, and 93.04%, respectively. The proposed DQ-NNPP method achieved 93.74% accuracy, which was 1.76% better than that of SAB-UAS, 0.7% better than that of the PPDP method, and only slightly worse (1.24%) than that of MSCryptoNet.

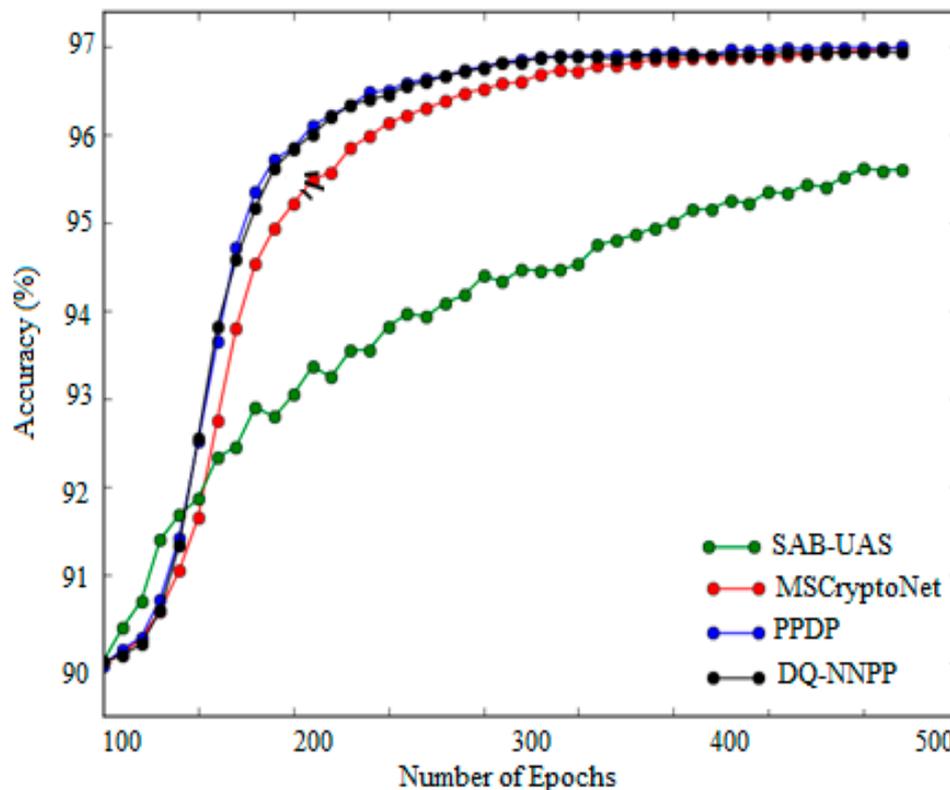


Figure 4. Comparison of accuracy.

Sensitivity estimates the efficiency of the scheduling model. It is measured as the probability of the positive prediction of identified features, and is also termed as the true-positive rate (TPR), as given in Equation (15):

$$\text{Sensitivity} = \frac{TP}{TP + FP} \tag{15}$$

Figure 5 illustrates the comparison of sensitivity between the SAB-UAS, MSCryptoNet, and PPDP methods, and the proposed DQ-NNPP method. The Xaxis presents the number of epochs utilized for the examination, and the Yaxis shows the sensitivity values acquired in percentages. The SAB-UAS, MSCryptoNet, and PPDP methods achieved sensitivity of 79.4%, 84.72%, and 86.42%, respectively. Comparatively, the proposed DQ-NNPP method achieved 92% sensitivity, which was 13.4%, 8.72%, and 6.42% better than those of SAB-UAS, MSCryptoNet, and PPDP, respectively.

Specificity is the probability of true negatives that are aptly identified, and is also termed true-negative rate (TNR). The formula for specificity is given in Equation (16):

$$\text{Specificity} = \frac{TP}{TP + FN} \tag{16}$$

Figure 6 compares the specificity of the existing SAB-UAS, MSCryptoNet, and PPDP methods, and of the proposed DQ-NNPPmethod, where the number of epochs used for analysis is given on the Xaxis, and specificity values obtained in percentages are on the Yaxis. The existing SAB-UAS, MSCryptoNet, and PPDP methods achieved specificity of 90.7%, 91.44%, and 91.58%, respectively. In comparison, the proposed DQ-NNPP method achieved 92.1% specificity, which was 2.6% better than that of SAB-UAS, 1.34% better than that of MSCryptoNet, and 1.48% better than that of the PPDP method.

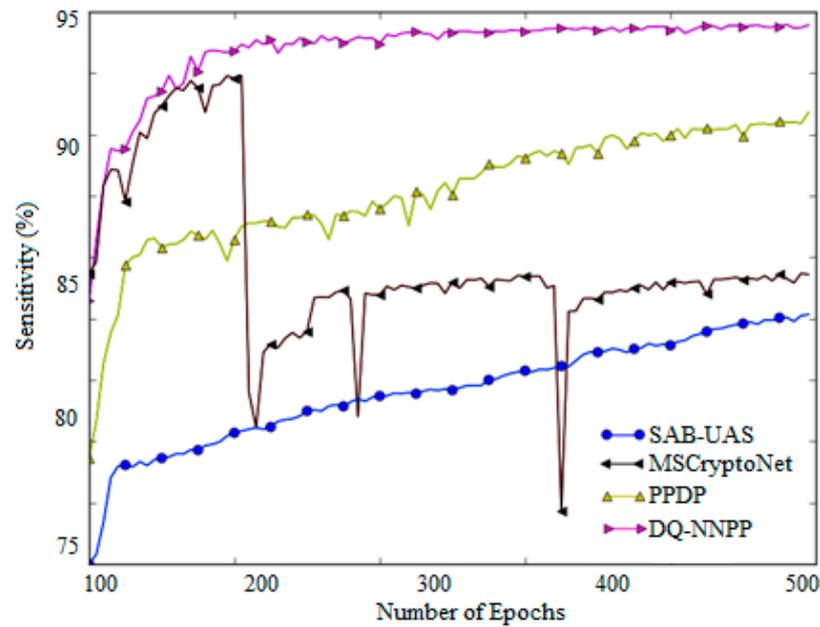


Figure 5. Comparison of sensitivity.

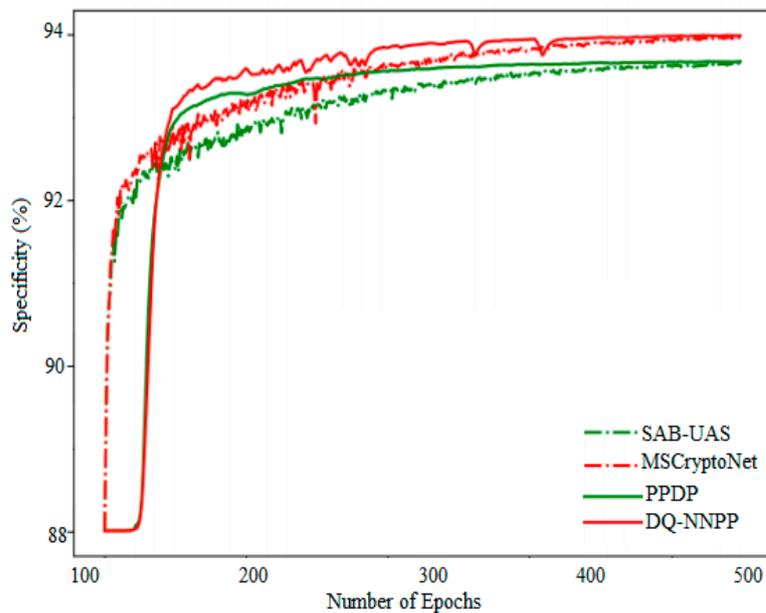


Figure 6. Comparison of specificity.

Communication overhead (C) is the ratio of the total packets (N_{pack}) transmitted from node x to node y in less time. The formula for communication overhead is given in Equation (17):

$$\sum_0^{N_{pack}} x \rightarrow y \tag{17}$$

Figure 7 illustrates the comparison of communication overhead between SAB-UAS, MSCryptoNet, PPDP, and the proposed DQ-NNPP method. The Xaxis displays the number of epochs utilized for analysis, and the Yaxis gives the communication overhead values obtained in percentages. The SAB-UAS, MSCryptoNet, and PPDP methods achieved a communication overhead 64.62%,65.24%, and 66.76%,respectively. In comparison, the proposed DQ-NNPP method achieved67.08% communication overhead, which was3.04%,

2.24%, and 2.3% better than those of the SAB-UAS, MSCryptoNet, and PPDP methods, respectively.

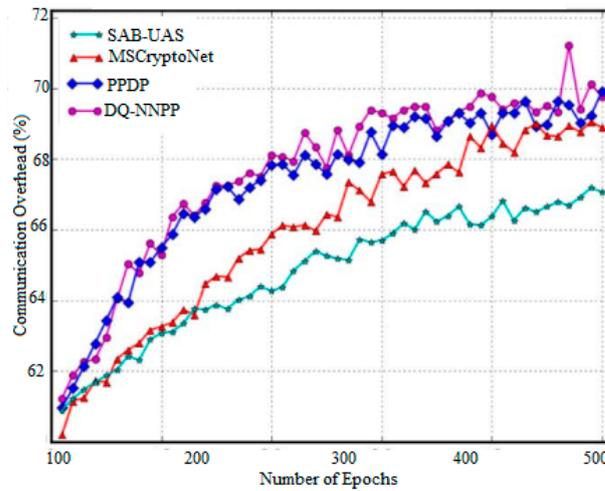


Figure 7. Comparison of communication overhead.

Time ofEncryption (E)is the time reserved by the algorithm for the conversion of plain text (P) into cipher text (C) using asymmetric or asymmetric keys. The formula for encryption time is defined in Equation (18):

$$E = \text{Time}(P \rightarrow C) \tag{18}$$

Figure 8 presents the encryption time comparison between the existing methods and the proposed method, in which the number of epochs used for analysis is given on the Xaxis, and the encryption time values in milliseconds are on the Yaxis. When compared, the existing SAB-UAS, MSCryptoNet, and PPDP methods achieved encryption times of 64, 62.2, and 60.52 ms, respectively. Comparatively, the proposed DQ-NNPP method achieved an encryption time of 58.72 ms, which was 6.72, 4.4, and 2.3 ms faster than those of the SAB-UAS, MSCryptoNet, and PPDP methods, respectively.

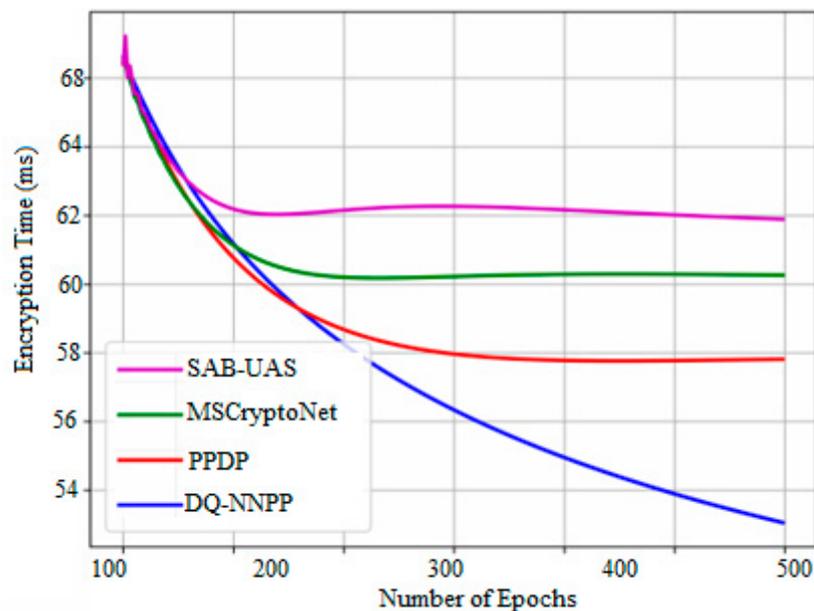


Figure 8. Comparison of encryption time.

Time of Decryption (D) is the time engaged by an algorithm for the conversion of cipher text (P) into plain text (C) using asymmetric or asymmetric keys. The formula for encryption time is provided in Equation (19):

$$D = \text{Time}(C \rightarrow P) \tag{19}$$

Figure 9 presents the decryption time comparison between the existing SAB-UAS, MSCryptoNet, and PPDP methods, and the proposed DQ-NNPP method. The Xaxis displays the number of epochs used for analysis, and the Yaxis gives the decryption time values obtained in milliseconds. The existing SAB-UAS, MSCryptoNet, and PPDP methods achieved decryption times of 67.48, 66.58, and 64.74, respectively. In comparison, the proposed DQ-NNPP method achieved a decryption time of 62.72 ms, which was 5.36 ms faster than that of SAB-UAS, 4.5 ms faster than that of MSCryptoNet, and 2.02 ms faster than that of the PPDP method. Table 1 provides the overall comparative analysis of all methods.

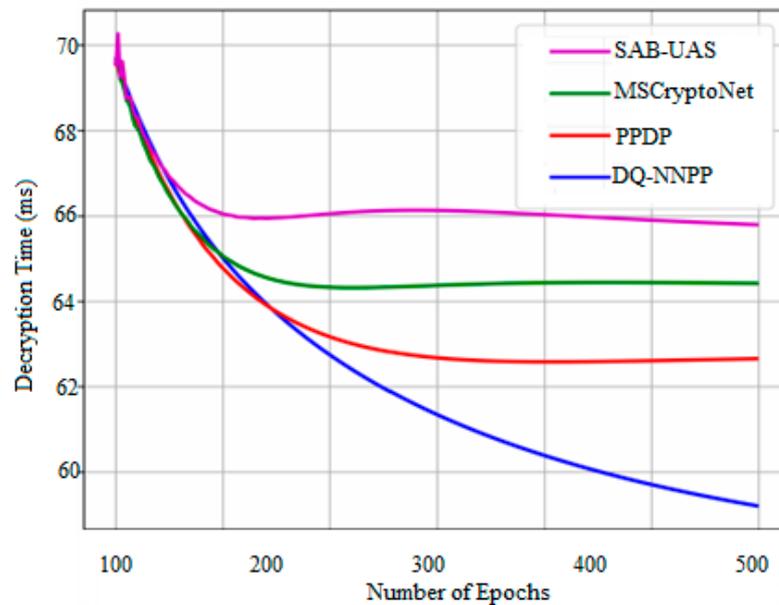


Figure 9. Comparison of decryption time.

Table 1. Overall comparison between proposed and existing methods.

Parameters	SAB-UAS [12]	MSCryptoNet [14]	PPDP [16]	DQ-NNPP (Proposed)
Accuracy (%)	92.02	94.3	93.04	93.74
Sensitivity (%)	79.4	84.72	86.42	92
Specificity (%)	90.7	91.44	91.58	92.1
Communication Overhead (%)	64.62	65.24	66.76	67.08
Encryption time (ms)	64	62.2	60.52	58.72
Decryption time (ms)	67.48	66.58	64.74	62.72

5. Conclusions

Security and privacy are the most challenging issues in IoT healthcare applications. With limited resources in IoT, existing security approaches are not appropriate. The proposed deep Q-learning-based neural network with privacy preservation method (DQ-NNPP) architecture overcomes the challenges of security and privacy threats. This paper introduced novel ciphertext-policyattribute-based privacy preservation (CPABPP), which combines the benefits of private, public, and master keys for designing a patient-centric access control approach used in electronic medical sectors, thereby ensuring security and privacy. The proposed method demonstrated superior results when compared with the existing SAB-UAS, MSCryptoNet, and PPDP methods, achieving 93.74% accuracy, 92% sensitivity, 92.1% specificity, 67.08% communication overhead, encryption time of 58.72 ms, and decryption time of 62.72 ms. Future works should also include nonoptimized data searching in a deep-learning concept to improve security.

Author Contributions: Drafting, N.D.K.; collect the dataset, A.C.; proof reading and experimental analysis, N.I. and M.R.; propose the new method or methodology, A.H.G. All authors have read and agreed to the published version of the manuscript.

Funding: No fund has been received for the completion of this research work.

Data Availability Statement: Data will be shared for review based on the editorial reviewer's request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Buttyan, L.; Hubaux, J.P. Privacy protection. In *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*; Cambridge University Press: New York, NY, USA, 2008; pp. 237–254.
2. Ramos, J.L.H.; Bernabe, J.B.; Skarmeta, A.F. Towards Privacy-preserving data sharing in smart environments. In Proceedings of the IEEE 8th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Birmingham, UK, 2–4 July 2014; pp. 334–339.
3. Gue, X.; Duan, X.; Gao, H.; Huang, A.; Jiao, B. An ECG Monitoring and Alarming System Based on Android Smart Phone. *Commun. Netw.* **2013**, *5*, 584–589. [[CrossRef](#)]
4. Sonar, K.; Upadhyay, H. A Survey: DDOS Attack on Internet of Things. *Int. J. Eng. Res. Dev.* **2014**, *10*, 58–63.
5. Miao, Y.; Ma, J.; Liu, X.; Wei, F.; Liu, Z.; Wang, X.A. m2-ABKS: Attribute-Based Multi-Keyword Search over Encrypted Personal Health Records in Multi-Owner Setting. *J. Med. Syst.* **2016**, *40*, 68. [[CrossRef](#)] [[PubMed](#)]
6. Huang, M.; Liu, A.; Wang, T.; Huang, C. Green data gathering under delay differentiated services constraint for internet of things. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 9715428. [[CrossRef](#)]
7. Rahim, R.; Murugan, S.; Mostafa, R.R.; Dubey, A.; Regin, K.; Kulkarni, R.; Dhanalakshmi, V. Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords. *Webology* **2020**, *17*, 524–535. [[CrossRef](#)]
8. Tang, J.; Liu, A.; Zhao, M.; Wang, T. An Aggregate Signature Based Trust Routing for Data Gathering in Sensor Networks. *Secur. Commun. Netw.* **2018**, *2018*, 6328504. [[CrossRef](#)]
9. Al-Qatf, M.; Lasheng, Y.; Al-Habib, M.; Al-Sabahi, K. Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection. *IEEE Access* **2018**, *6*, 52843–52856. [[CrossRef](#)]
10. Otoum, S.; Kantarci, B.; Mouftah, H.T. On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Netw. Lett.* **2019**, *1*, 68–71. [[CrossRef](#)]
11. Ahamad, D.; Alam Hameed, S.; Akhtar, M. A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. *J. King Saud Univ.-Comput. Inf. Sci.* **2020**. [[CrossRef](#)]
12. Deebak, B.D.; Al-Turjman, F.; Aloqaily, M.; Alfandi, O. An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT. *IEEE Access* **2019**, *7*, 135632–135649. [[CrossRef](#)]
13. Wang, K.; Chen, C.-M.; Tie, Z.; Shojafar, M.; Kumar, S.; Kumari, S. Forward Privacy Preservation in IoT enabled Healthcare Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1991–1999. [[CrossRef](#)]
14. Kwabena, O.A.; Qin, Z.; Zhuang, T.; Qin, Z. Mscryptonet: Multi-scheme privacy-preserving deep learning in cloud computing. *IEEE Access* **2019**, *7*, 29344–29354. [[CrossRef](#)]
15. Keshavarzian, A.; Sharifian, S.; Seyedin, S. Modified deep residual network architecture deployed on serverless framework of IoT platform based on human activity recognition application. *Futur. Gener. Comput. Syst.* **2019**, *101*, 14–28. [[CrossRef](#)]
16. Zhang, C.; Zhu, L.; Xu, C.; Lu, R. PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system. *Futur. Gener. Comput. Syst.* **2018**, *79*, 16–25. [[CrossRef](#)]
17. Veeramakali, T.; Siva, R.; Sivakumar, B.; Mahesh, S.P.; Krishnaraj, N. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. *J. Super Comput.* **2021**, *77*, 1–21. [[CrossRef](#)]

18. Hui, H.; Zhou, C.; Xu, S.; Lin, F. A novel secure data transmission scheme in industrial internet of things. *China Commun.* **2020**, *17*, 73–88. [[CrossRef](#)]
19. Liang, W.; Tang, M.; Long, J.; Peng, X.; Xu, J.; Li, K.-C. A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3582–3592. [[CrossRef](#)]
20. Abirami, P.; Bhanu, S.V. Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment. *Soft Comput.* **2020**, *24*, 18927–18936. [[CrossRef](#)]
21. Zhang, L.; Shi, Y.; Chang, Y.-C.; Lin, C.-T. Hierarchical Fuzzy Neural Networks with Privacy Preservation for Heterogeneous Big Data. *IEEE Trans. Fuzzy Syst.* **2020**, *29*, 46–58. [[CrossRef](#)]
22. Bi, H.; Liu, J.; Kato, N. Deep Learning-based Privacy Preservation and Data Analytics for IoT Enabled Healthcare. *IEEE Trans. Ind. Inform.* **2021**. [[CrossRef](#)]
23. Zhu, J.; Song, Y.; Jiang, D.; Song, H. A new deep-Q-learning-based transmission scheduling mechanism for the cognitive Internet of Things. *IEEE Internet Things J.* **2017**, *5*, 2375–2385. [[CrossRef](#)]
24. Yang, L.; Yu, K.; Yang, S.X.; Chakraborty, C.; Lu, Y.; Guo, T. An Intelligent Trust Cloud Management Method for Secure Clustering in 5G enabled Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2021**. [[CrossRef](#)]
25. Liu, J.; Liu, H.; Chakraborty, C.; Yu, K.; Shao, X.; Ma, Z. Cascade Learning Embedded Vision Inspection of Rail Fastener by Using a Fault Detection IoT Vehicle. *IEEE Internet Things J.* **2021**. [[CrossRef](#)]
26. Guesmi, R. A novel design of Chaos based S-Boxes using genetic algorithm techniques. In Proceedings of the 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA), Doha, Qatar, 10–13 November 2014.
27. Qin, Q.; Jin, B.; Liu, Y. A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain. *BioMed Res. Int.* **2021**, *2021*, 6676171. [[CrossRef](#)] [[PubMed](#)]