electronics

MDPI

Article

Secure Healthcare Model Using Multi-Step Deep Q Learning Network in Internet of Things

Patibandla Pavithra Roy [1], Ventrapragada Teju [1], Srinivasa Rao Kandula [1], Kambhampati Venkata Sowmya [2], Anca Ioana Stan [3] and Ovidiu Petru Stan [4,5,*]

[1] Department of Electronics & Communications Engineering, Dhanekula Institute of Engineering and Technology, Vijayawada 521139, India; drpavithraroy@diet.ac.in (P.P.R.); ventrapragadateju@diet.ac.in (V.T.); ksrinivas.ece@diet.ac.in (S.R.K.)

[2] Department of Electronics & Communications Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, India; sowmyakambhampati@kluniversity.in

[3] Faculty of Industrial Engineering, Robotics and Production Management, Technical University of Cluj Napoca, 400114 Cluj Napoca, Romania; anca.stan@muri.utcluj.ro

[4] OSEAN—Outermost Regions Sustainable Ecosystem for Entrepreneurship and Innovation, University of Madeira Colégio dos Jesuítas, 9000-082 Funchal, Portugal

[5] Faculty of Automation and Computer Science, Technical University of Cluj Napoca, 400114 Cluj Napoca, Romania

* Correspondence: ovidiu.stan@aut.utcluj.ro

Abstract: Internet of Things (IoT) is an emerging networking technology that connects both living and non-living objects globally. In an era where IoT is increasingly integrated into various industries, including healthcare, it plays a pivotal role in simplifying the process of monitoring and identifying diseases for patients and healthcare professionals. In IoT-based systems, safeguarding healthcare data is of the utmost importance, to prevent unauthorized access and intermediary assaults. The motivation for this research lies in addressing the growing security concerns within healthcare IoT. In this proposed paper, we combine the Multi-Step Deep Q Learning Network (MSDQN) with the Deep Learning Network (DLN) to enhance the privacy and security of healthcare data. The DLN is employed in the authentication process to identify authenticated IoT devices and prevent intermediate attacks between them. The MSDQN, on the other hand, is harnessed to detect and counteract malware attacks and Distributed Denial of Service (DDoS) attacks during data transmission between various locations. Our proposed method's performance is assessed based on such parameters as energy consumption, throughput, lifetime, accuracy, and Mean Square Error (MSE). Further, we have compared the effectiveness of our approach with an existing method, specifically, Learning-based Deep Q Network (LDQN).

Keywords: deep learning network; distributed denial of service attack; healthcare system; internet of things; malware attacks; multi-step deep Q learning network

check for updates

Citation: Roy, P.P.; Teju, V.; Kandula, S.R.; Sowmya, K.V.; Stan, A.I.; Stan, O.P. Secure Healthcare Model Using Multi-Step Deep Q Learning Network in Internet of Things. *Electronics* **2024**, *13*, 669. https://doi.org/10.3390/electronics13030669

Academic Editor: Andreas Mauthe

Received: 1 December 2023
Revised: 17 January 2024
Accepted: 1 February 2024
Published: 5 February 2024

1. Introduction

Internet of Things (IoT) is a vast global infrastructure that integrates various components, including physical or virtual objects with attributes, Auto-IDs, and self-configuration capabilities in standard communication systems [1]. Through IoT, devices such as smartphones, physical sensors, and smart buildings can interconnect and exchange data seamlessly, utilizing both wired or wireless communication channels [2]. Within the context of Industry 4.0, which focused on enhancing industrial environments [3], the integration of Cyber-Physical Systems (CPS) and IoT is gaining momentum, particularly in electrical systems and machinery. One notable development is the emergence of machine learning (ML)-based IoT platforms designed to mitigate cyber-attacks while ensuring secure and reliable status monitoring of devices like induction motors. Additionally, IoT is revolutionizing traditional methods of observation, for example by introducing a unique IoT architecture for real-time monitoring of gas-insulated switchgear [4]. This convergence not only offers exciting possibilities, like real-time monitoring and enhanced cybersecurity, but also plays a significant role in modernizing electric power plants [5]. In today's world, ML methods have proven effective for addressing issues like chatter recognition across various applications.

The exceptional performance of chatter classification is primarily attributed to the utilization of ML techniques [5]. These techniques are commonly used for signal classification and analysis. In contrast to conventional chatter detection systems, a recent innovation has introduced a data fusion approach that relies on multiple sensor inputs for milling chatter detection. This method is cost-effective and straight forward to implement, using microphone and accelerometer sensors to monitor chatter during milling operations. In order to enhance the accuracy of the chatter detection system, a novel approach introduces fuzzy entropy alongside hybrid feature selection, accompanied by a similarity classifier [6]. This multifaceted technique demonstrates its efficacy in addressing the issue of chatter in the machining process.

In the realm of cybersecurity, researchers like Mahmoud Elsisi and Minh-Quang Tran [7] have developed trustworthy, safe, and secure online monitoring for autonomous guided vehicles (AGVs). Their approach features a deep neural network (DNN) with a rectified linear unit, replacing outdated detection methods for cyber-attacks. In order instance, Mahmoud Elsisi et al. have designed and developed an IoT architecture that integrates deep learning for online monitoring of power transformers and protection against cyber-attacks [8]. For the purpose of diagnosing power transformer faults and addressing cyber threats, they leverage a one-dimensional convolutional neural network (1D-CNN).

- Using IoT, patient care can be facilitated.
- Integrating IoT and deep learning provides better monitoring of patients, providing privacy and security.
- In this research work, a secure healthcare model is introduced using Multi-Step Deep Q Learning Network with IoT.
- MSDQN is combined with DLN to improve the privacy and security of healthcare data.

In recent studies, researchers have used technology to develop products that enhance the quality of care for both patients and clinicians by utilizing industry expertise and human-centered design principles. The emergence of IoT-driven healthcare applications represents a notable advancement in this field, with the potential to improve the quality of patient care while simultaneously cutting costs [9]. One remarkable extension of IoT is into the field of biomedicine. This expansion involves the deployment of sensors, often via wearable technology, directly at the patients' end. These sensors can seamlessly communicate with hospitals and emergency response systems, ensuring immediate data transmission if necessary [10].

The rest of the paper is organized as follows

- Section 2 describes related work
- Section 3 discusses the methodology
- Section 4 discusses the results and performance analysis
- Section 5 presents the conclusion of the paper

2. Related Work

In [11], the authors discussed layered architecture, comprising multiple levels such as the Application Layer, Communication Layer, Security Layer, Embedded Layer, Hardware Layer, Integration Layer, and DB Layer, which has been recognized as the most effective method for achieving effective communication among devices connected to the Internet. IoT devices are capable of producing diverse forms of data, including text, photos, audio files, and videos [12]. This versatility in IoT technology has opened doors to a wide array of services and applications, encompassing smart traffic management, efficient parking solutions, intelligent lighting systems, smart offices, and sophisticated vehicle control [13].

Smart devices play a critical role in assessing a patient's health status by collecting data on parameters like temperature, blood pressure, heart rate, and saline bottle level [14]. Medical sensors now offer a solution for various medical applications, such as remote patient activity monitoring, patient information management, chronic illness diagnosis, and elderly healthcare [15,16]. Despite the potential benefits, the adoption of IoT in medical systems faces several challenges. IoT devices are often resource-constrained and deployed in unmonitored, physically vulnerable locations, necessitating the development of a secure IoT architecture [17]. Patient medical information, stored on servers, remains a prime target for hackers because of its sensitivity, emphasizing the need for secure communication between IoT devices and servers [18]. To address these concerns, a two-dimensional IoT architecture and framework (as depicted in Figure 1) has been designed to ensure end-to-end security. IoT operates across three levels, perception, network, and application, with data flowing through these layers. Each layer presents unique security challenges, including issues related to confidentiality, integrity, and authenticity, often influenced by human interaction.

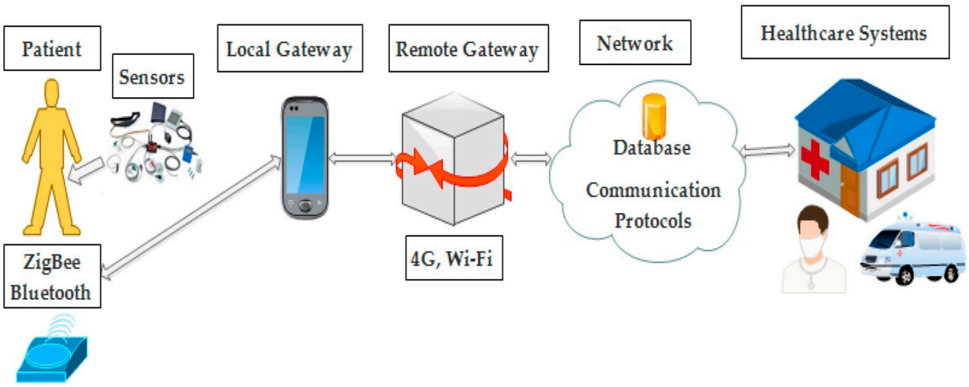

Figure 1. Flow of data through Perception, Network, and Application layers.

In the development of secure IoT healthcare systems, a combination of various methods is employed, including the lightweight SIMON block cypher [19], the lightweight SIMON-based cryptography algorithm [20], the self-healing mechanism [21], and other standard methods.

Yeh [22] demonstrated the IoT-based communication architecture using three crucial parts: Body Sensor Networks (BSN) server, wearable body biosensors, and local processing units (LPU). This IoT design involves two channels of communication: sensors to LPU, and LPU to BSN server. The openness of these channels possesses potential security risks. To solve this, the communication process is divided into two distinct phases: initialization and authentication. During the initialization phase, security parameters are exchanged between the communication entities. Authentication is established between LPU and BSN, as well as between exchanged LPU, enhancing the transmission security and secrecy. Deebak et al. [23] created a system that enhances security and anonymity in smart electronic healthcare applications through Secure and Anonymous-Based User Authentication System (SAB-UAS). SAB-UAS addresses the long-standing challenge of usability-security trade-offs by implementing a systematic framework involving key communication stakeholders: medical experts, wireless gateways, and biomedical sensors. It is worth mentioning that SAB-UAS demonstrates higher throughput when the network has a larger number of nodes.

Another noteworthy advancement in healthcare security is the use of blockchain technology, as presented by Rathee et al. [24]. By hashing each piece of data, they create a secure foundation. This approach addresses concerns related to medications hacking and data tampering. Blockchain technology proves particularly effective in enhancing transparency and security in healthcare supply chains and document access. However, challenges remain in implementing blockchain technology within healthcare institutions.

Sharma and Kalra [25] have developed a lightweight user authentication mechanism for remote patient monitoring. Their approach encompasses six different phases, including: framework setup (selecting a secret key for the gateway node, establishing the initial configuration); registration of medical practitioner; registration of patient; login and authentication; and password update. During the login and authentication phase, medical professionals retrieve the patients' medical records, and mutual authentication occurs between the gateway node, medical practitioners, and sensors. A unique random session key is generated [26]. For managing privacy and security in IoT-based healthcare systems, Shakeel et al. [27] introduced a powerful technique based on machine learning, known as the Learning-based Deep-Q-Network (LDQN) approach. The increasing attention of researchers has led to the emergence of IoT into the healthcare sector, where there are multiple innovations being done. Due to this emergence, it has made human lives more secure and less prone to diseases [28,29]. In [30], the author discusses the deep Q learning based neural network with a privacy preservation method, DQNNPP. In this a model for secure transmission of healthcare data, known as EDBN—Enhanced Dynamic Bayesian Network—is discussed [31]. In [32], a demonstration of IoT architecture based on improving the deep learning model known as YOLO—You Only Look Once—for providing security is given.

In this research, a model for knowing an individual's health condition and providing proper medication is designed [33]. In [34], an approach for an IoT healthcare monitoring system and enhanced IGWO (Improved Grey-Wolf Optimization)-based DCNN (Deep Convolution Neural Network) model to detect lung cancer is discussed.

In [35], a proposed model known as ICBS (Information Centric Dissemination Scheme) for smart cities to provide smart health is discussed. Jyothi Peta and Srinivas Koppu [36] introduced SPWO (Student Psychology Whale Optimization)-based deep max out network. It classifies breast cancer disease. In [37], a review on various deep learning techniques for IoT information is discussed.

Figure 2 depicts the various processing steps involved in LDQN. This ML method is used to examinate problems related to access control, authentication, and virus detection. Additionally, employing LDQN eliminates intermediate attacks, like spoofing attacks. The LDQN approach has been developed and applied to maintain the integrity, security, and privacy of health reports and data transfers. Specifically, LDQN is instrumental in detecting and blocking malware threats during the transmission of health-related information. This ensures that health data remain safe, reliable, and protected during the process of generating health reports or transferring information.

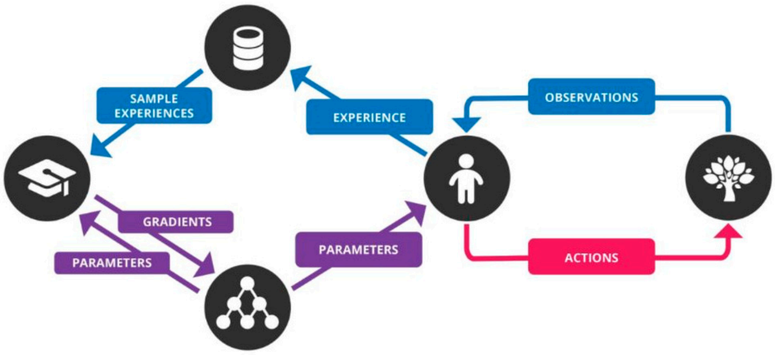

Figure 2. Architecture of Deep Q- Learning Algorithm.

3. Methodology

To ensure the security of IoT healthcare data against malware attack, DDoS attack, and intermediate attacks, the proposed method leverages deep learning algorithms, specifically DLN and MSDQN. The proposed approach comprises two distinct phases: access control and authentication. In the first phase, the authentication method is developed using DLN to identify an authenticated IoT device and prevent intermediate attacks. This step is crucial in establishing the integrity of the IoT network. In the second phase, MSDQN is utilized to secure the transfer of healthcare data through IoT devices. Figure 3 provides a visual representation in the form of a block diagram, illustrating the components and flow of the proposed approach.

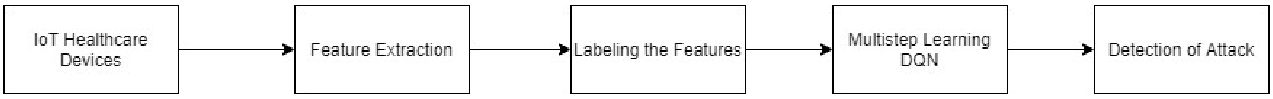

Figure 3. Block diagram of the proposed method.

The main contributions of this research paper can be summarized as follows: (a) Deep Learning Network for intermediate attacks and IoT device authentication—it leverages a deep learning network that utilizes signal features, including the received signal strength, impulse response of the channel, state information of the channel, and received signal strength indicator, to address intermediate attacks and authenticate IoT devices; (b) MSDQN for identifying malware and DDoS attacks—by analyzing traffic attributes and signal features using MSDQN, malware, and DDoSattacks can be identified during data transmission; (c) Reducing data leakage in medical data transmission—by combining DLN and MSDQN, we offer a comprehensive approach to safeguarding the integrity and privacy of medical data.

3.1. Authentication Using Deep Learning Network Existing Designs (or Original Designs)

In the proposed method, authentication is considered the initial and critical step for ensuring the secure transfer of health information between IoT devices. The IoT devices used in this proposed technique have limited memory sources, which poses challenges for a robust authentication process. To enhance the security and privacy of the transmitted information, various signal features, such as the received signal strength, impulse response of the channel, state information of the channel, and received signal strength indication, are used. However, the resource constraints associated with IoT devices can inhibit the effectiveness of the authentication mechanism during the transmission of healthcare data. These limitations underscore the need for efficient and resource-friendly authentication methods to maintain data privacy in IoT healthcare systems.

3.2. Deep Learning Network (DLN)

This proposed method takes advantage of the DLN to overcome the authentication challenges arising from the resource limitations. In IoT networks, the limited battery and memory capacity often give rise to Sybil attacks. To counter these vulnerabilities, the effective learning of IoT device features is implemented at every level. Consequently, the proposed approach for transmitting healthcare data integrates DLN within IoT devices. This integration not only reinforces the authentication but also significantly reduces the risk of data leakage during transmission.

IoT devices, such as sensors and actuators were subjected to testing within predefined range boundaries. To verify the privacy of data transmission, an authentication request is initiated from one IoT device to another positioned within the designated testing area. The authentication request is then processed, which involves the extraction of several signal properties. These properties include the signal strength, impulse response of the channel, channel state information, and received signal strength indication, all within a specific range. DLN evaluates ambient radio signals and packet request arrival times based on these extracted features. The acquired features, obtained during the DLN training procedure, are then used to determine the appropriate output for the authentication process. To ensure an effective DLN training, Adaboost training is used, even when the features contain noise or errors. Equation (1) shows the feature training process of the DLN.

$$f(y) = \sum_{k=1}^{k} \alpha_k h_k(y), \tag{1}$$

In the pooling layer, the features are represented as α_k and the more refined features are denoted as h_k. These trained features are then stored in a database and are utilized to carry out the authentication process. For any new device seeking authentication, an analysis of signal features is performed. The analysis relies on the input, hidden, and output layers, which constitute the three fundamental layers of DLN. Moreover, specific bias value c and weight values w_j are used in the above-mentioned layer during the evaluation of the authentication output, as illustrated in Equation (2).

$$N_o = \sum_{j=1}^{M} y_j \, * \, w_j + c, \tag{2}$$

In the estimation phase of the authentication result, the Levenberg–Marquardt learning algorithm plays a significant role in further training the DLN. As shown in Equation (3), the weights and bias values are updated using the Levenberg–Marquardt approach for an accurate and efficient authentication process:

$$Y_{l+1} = Y_l \; - \; \left[K^T K + \mu J\right]^{-1} K^T e, \tag{3}$$

where:

- K is the Jacobian matrix
- μ is the combination coefficient
- e is the error vector.

As a result, the training features are compared to incoming authentication requests to authenticate the IoT devices. This DLN-based authentication mechanism effectively eliminates intermediary attacks during the transmission of healthcare data. Furthermore, following the authentication procedure, a multi-step Q learning mechanism is used to enhance the security of medical data during the transmission process.

3.2.1. MSDQN-Based Secure Data Transmission of IoT Healthcare Data

The final step of the proposed method focuses on securing the transmission of the medical healthcare data through the utilization of the MSDQN. The DLN-based authentication process is used to analyze traffic requests related to medical data. In this verification process, various traffic parameters, including host post number, frame length, transmitting protocols, frame number, transmitting file type, and request IP address, are examined. These traffic parameters, along with signal attributes like the received signal strength, channel impulse response, channel status data, and received signal strength indication, are stored in a database. When transmitting IoT healthcare data, the features from the database are used to train MSDQN, enabling it to effectively detect and mitigate malware and DDoS attacks.

3.2.2. Multi-Step Deep Q Learning Network Algorithm

The function of new state–action value $\hat{Q}^{\pi}(s,b)$ is modified when the agent proceeds action b in state s under policy of π. The function of new state–action value is expressed in the Equation (4).

$$\hat{Q}^{\pi}(s,b) = E_{\pi}\left[\hat{G}_t(m) \middle| s_t = s, b_t = b\right] b, \tag{4}$$

The return function $\hat{G}_t(m)$ is modified based on the Markov property that is illustrated in the Equation (5).

$$\hat{G}_t(m) = \hat{r}_t(m) + \gamma \widehat{G_{t+1}}(m), \tag{5}$$

where $\hat{r}_t^{(m)} = \frac{1}{m}\sum_{l=1}^{l=m} r_{(t+l-1)}$. Additionally, the new state function value of Equation (4) is calculated, along with dynamic programming which is expressed in the Equation (6).

$$\hat{Q}(s,b) = E_\pi\left[\hat{r}_t(m) + \gamma E_{b'}\hat{Q}^{\wedge}(s',b')\middle|s_t = s, b_t = b\right] \tag{6}$$

where, $s\prime$ is the subsequent state of state s based on the state transition probability. Similar to the conventional Q learning, the backup operation is used to estimate the new optimal state–action value function which is expressed in Equation (7).

$$\hat{Q}(s_t,b_t) \leftarrow \hat{Q}(s_t,b_t) + \alpha\left[\hat{r}_t^{(m)} + \gamma \max_b \hat{Q}(S_{t+1},b) - \hat{Q}(S_t,b_t)\right], \tag{7}$$

The MSDQN uses the reward $\hat{r}_t^{(m)}$ instead of r_t when compared to the one-step temporal difference method. The function of the new state–action value $\hat{Q}(s,b)$ is approximated by using a parameterized continuous function $\hat{Q}(s,b;\theta)$ for a continuous state space problem.

Therefore, the authentication process using DLN avoids the intermediate attacks between the IoT devices. The DLN is used to identify whether the IoT device is authenticated or not, based on trained features. Then MSDQN is used to maintain the security, privacy, and reliability of the data transmission and also detects the DDoS, malware affected health data.

4. Results and Discussions

This section provides an overview of the experimental results and an explanation of the proposed method's implementation. The identification of attacks in the IoT-based healthcare system is carried out through implementation and simulation in Python, using Open Flow environment with 4 GB RAM and i5 processor. The specifications considered in this proposed method are given in the Table 1. The IoT devices responsible for healthcare data transmission are deployed within an area of 250 m^2 featuring a varying number of nodes (i.e., 50, 60, 80, 90 nodes). Moreover, these IoT devices use a log-shadowing wireless model as their channel mode.

Table 1. Graph representations.

Parameters	Values
Area	250 m^2
Number of nodes	50, 60, 70, 80, 90
MAC	IEEE 802.5.14
Transmission	250 kbps
Packet size	40 bytes
Simulation time	400

4.1. Performance Measures' Indicators

The performance of the proposed method is assessed through various key metrics, including energy consumption, throughput, lifetime, accuracy, and mean Square Error (MSE) for attack detection. These performance measures are described as follows:

- Energy consumption—this metric quantifies the amount of energy consumed by IoT devices for transmitting data over the network. The energy consumption is directly proportional to the distance between the devices;
- Throughput—is defined as the number of bits transmitted from one location to another, typically expressed in bits per second;
- Lifetime—represents the duration until all devices within the network die during data transmission. An IoT device is declared "dead" when it lacks the energy required for data transmission;

- Accuracy—in the context of malware and DDoS attack detection during healthcare data transmission is defined as the ratio of correctly predicted observations to the total number of observations. It is computed using the formula:

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN}, \tag{8}$$

where, *TP* is true positive, *TN* is true negative, *FP* is false positive, and *FN* is false negative.

- MSE—quantifies the amount of error caused by attacks on the IoT-based healthcare system. It is computed as:

$$\text{MSE} = \frac{1}{\text{N}_\text{D}} \sum\nolimits_{\text{j}=1}^{\text{N}_\text{D}} \left(\text{I}_\text{P} - \hat{\text{I}}_\text{P}\right)^2, \tag{9}$$

where, MSE is mean Square Error, N_D is number of data points, I_P is actual input and $\hat{I}_P$ is output acquired through IoT communication.

4.2. Performance Analsys

This section provides a detailed analysis of the performance of the proposed method, evaluated using two classifiers, Q Learning Network (QLN) and Deep Q Network (DQN). These classifiers are used instead of the MSQDN for malware and DDoS attack detection. The evaluation encompasses the same specification mentioned in Table 1. The performance of the proposed method is assessed by conducting simulations with varying numbers of IoT devices deployed within the test area. Specifically, the IoT devices are varied in number, ranging from 50 to 90.

Tables 2–6 show the performances of the proposed method for 50, 60, 70, 80 and 90 IoT devices, respectively. Upon reviewing these tables, it becomes evident that the proposed method consistently outperforms QLN and DQN across various key performance metrics, including energy consumption, throughput, lifetime, accuracy, and error rate. For instance, the energy consumption of the proposed method with 90 IoT devices is 38 J, a notable improvement compared to QLN and DQN. This low energy consumption translates to an extended lifetime for the proposed method. Moreover, the proposed method demonstrates a high classification ratio of 99.39% for malware and DDoS attack detection with 80 IoT devices, surpassing QLN and DQN. This higher classification ratio significantly enhances the system's ability to effectively detect and prevent malware and DDoS attacks during healthcare data transmission across the IoT-based system.

Table 2. Performance analysis of proposed method for 50 IoT devices.

Parameters	QLN	DQN	Proposed Method
Energy consumption (J)	40	33	25
Throughput (bps)	1010	1280	1565
Lifetime (s)	256	282	373
Accuracy (%)	90.46	94.58	99.04
MSE	0.58	0.44	0.11

Table 3. Performance analysis of proposed method for 60 IoT devices.

Parameters	QLN	DQN	Proposed Method
Energy consumption (J)	43	36	28
Throughput (bps)	1050	1320	1565
Lifetime (s)	276	299	378
Accuracy (%)	92.78	96.42	99.24
MSE	0.75	0.38	0.08

Table 4. Performance analysis of proposed method for 70 IoT devices.

Parameters	QLN	DQN	Proposed Method
Energy consumption (J)	54	42	32
Throughput (bps)	1070	1324	1578
Lifetime (s)	287	310	388
Accuracy (%)	90.45	94.51	99.12
MSE	0.95	0.54	0.09

Table 5. Performance analysis of proposed method for 80 IoT devices.

Parameters	QLN	DQN	Proposed Method
Energy consumption (J)	61	49	36
Throughput (bps)	1135	1355	1590
Lifetime (s)	291	318	393
Accuracy (%)	91.62	92.78	99.39
MSE	0.83	0.72	0.08

Table 6. Performance analysis of proposed method for 90 IoT devices.

Parameters	QLN	DQN	Proposed Method
Energy consumption (J)	71	56	38
Throughput (bps)	1190	1420	1620
Lifetime (s)	308	332	398
Accuracy (%)	91.62	92.78	99.52
MSE	0.78	0.42	0.09

4.3. Comparative Analysis

The performance of the proposed method is compared with LDQN [20] to determine its effectiveness. In [20], there are two different phases, authentication and access control. The DLN is used for authenticating the IoT device and also it avoids the intermediate attacks. Subsequently, the LDQN is used in that to detect malware and DDoS attack during the health care data transmission from one place to another place.

Table 7 shows the comparative analysis of LQDN [20] and proposed method in terms of energy, throughput, lifetime, average accuracy, and MSE for 90 IoT devices. From the analysis, we conclude that the performances of the proposed method are better than the LDQN [20]. For example, the malware and DDoS attack detection using MSDQN achieves an average accuracy of 96.26%, better than the LDQN [20]. Moreover, the energy consumption of the proposed method is 38 J, which is less when compared to the LDQN, that leads to improving the network lifetime and throughput. The throughput and lifetime of the proposed method with 90 IoT devices are 1620 bps and 398 s respectively.

Table 7. Comparative analysis of the proposed method with LDQN in terms of energy, throughput and lifetime.

Parameters	LDQN [20]	Proposed Method
Energy consumption (J)	42	38
Throughput (bps)	1599	1620
Lifetime (s)	395	398
Accuracy (%)	98.79	99.26
MSE	0.12	0.09

5. Conclusions

In this paper, the DLN verifies the IoT device as to whether it is an authenticated device or not and removes the intermediate attacks. The performances of proposed method are better than the conventional classifiers, such as QLN and DQN. The DLN uses four signal features to minimize data leakage, such as received strength of the signal, impulse response of the channel, state information of the channel and received signal strength indicator. Then the MSDQN uses the traffic features along with signal features for detecting the malware and DDoS attack during the data transmission. This helps to preserve the medical data from malware and DDoS attack. In the proposed method, the energy consumption is 38 J, throughput is 1620 bps, lifetime is 398 s, MSE is 0.09. The accuracy of the proposed method with 60 IoT devices is 99.24%, which is high when compared to the QLN and DQN. Moreover, the proposed method accuracy of attack detection is 99.26%, which is high when compared to the LDQN. To improve the accuracy of the current technique, future study should include non-optimized data searching in a deep learning concept.

The future scope of this research can be extended to IoT-assisted healthcare services by incorporating autonomous control and human—computer interface (HCI) technologies for ambient intelligence.

Author Contributions: Conceptualization, P.P.R. and V.T.; methodology, K.V.S. and S.R.K.; software, K.V.S.; validation, P.P.R., V.T., K.V.S., A.I.S. and O.P.S.; formal analysis, S.R.K., K.V.S. and O.P.S.; investigation, P.P.R. and S.R.K.; resources, V.T., K.V.S. and S.R.K.; data curation, A.I.S. and O.P.S.; writing—original draft preparation, P.P.R.,V.T., K.V.S., S.R.K., A.I.S. and O.P.S.; writing—review and editing, K.V.S., A.I.S. and O.P.S.; visualization, K.V.S.; supervision, V.T. and K.V.S.; funding acquisition, A.I.S. and O.P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in this article.

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

References

1. Yu, J.; Bang, H.-C.; Lee, H.; Lee, Y.S. Adaptive Internet of Things and Web of Things Convergence Platform for Internet of Reality Services. *J. Supercomput.* **2016**, *72*, 84–102. [CrossRef]
2. Yang, Y.; Zheng, X.; Tang, C. Lightweight Distributed Secure Data Management System for Health Internet of Things. *J. Netw. Comput. Appl.* **2017**, *89*, 26–37. [CrossRef]
3. Tran, M.-Q.; Elsisi, M.; Mahmoud, K.; Liu, M.-K.; Lehtonen, M.; Darwish, M.M.F. Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment. *IEEE Access* **2021**, *9*, 115429–115441. [CrossRef]
4. Elsisi, M.; Tran, M.-Q.; Mahmoud, K.; Mansour, D.-E.A.; Lehtonen, M.; Darwish, M.M.F. Towards Secured Online Monitoring for Digitalized GIS Against Cyber-Attacks Based on IoT and Machine Learning. *IEEE Access* **2021**, *9*, 78415–78427. [CrossRef]
5. Tran, M.-Q.; Liu, M.-K.; Elsisi, M. Effective multi-sensor data fusion for chatter detection in milling process. *ISA Trans.* **2022**, *125*, 514–527. [CrossRef] [PubMed]
6. Tran, M.-Q.; Elsisi, M.; Liu, M.-K. Effective feature selection with fuzzy entropy and similarity classifier for chatter vibration diagnosis. *Measurement* **2021**, *184*, 109962. [CrossRef]
7. Elsisi, M.; Tran, M.Q. Development of an IoT Architecture Based on a Deep Neural Network against Cyber Attacks for Au-tomated Guided Vehicles. *Sensors* **2021**, *21*, 8467. [CrossRef]
8. Elsisi, M.; Tran, M.Q.; Mahmoud, K.; Mansour, A.; Lehtonen, M.; Mohamed, M.F. Effective IoT-based deep learning platform for online fault diagnosis of power transformers against cyberattacks and data uncertainties. *Measurement* **2022**, *190*, 110686. [CrossRef]
9. Alabdulatif, A.; Khalil, I.; Yi, X.; Guizani, M. Secure Edge of Things for Smart Healthcare Surveillance Framework. *IEEE Access* **2019**, *7*, 31010–31021. [CrossRef]
10. Mohanty, S.P.; Kougianos, E.; Guturu, P. SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT. *IEEE Access* **2018**, *6*, 5939–5953. [CrossRef]
11. Manogaran, G.; Varatharajan, R.; Lopez, D.; Kumar, P.M.; Sundarasekar, R.; Thota, C. A New Architecture of Internet of Things and Big Data Ecosystem for Secured Smart Healthcare Monitoring and Alerting System. *Futur. Gener. Comput. Syst.* **2018**, *82*, 375–387. [CrossRef]
12. Onasanya, A.; Lakkis, S.; Elshakankiri, M. Implementing IoT/WSN based Smart Saskatchewan Healthcare System. *Wirel. Netw.* **2021**, *25*, 3999–4020. [CrossRef]

13. Onasanya, A.; Elshakankiri, M. Smart Integrated IoT Healthcare System for Cancer Care. *Wirel. Netw.* **2019**, *27*, 4297–4312. [CrossRef]
14. Nalajala, P.; Lakshmi, S.B. A Secured IoT Based Advanced Health Care System for Medical Field using Sensor Network.International. *J. Eng. Technol.* **2018**, *7*, 105–108.
15. Verma, P.; Sood, S.K.; Kalra, S. Cloud-Centric IoT based Student Healthcare Monitoring Framework. *J. Ambient. Intell. Humaniz. Comput.* **2018**, *9*, 1293–1309. [CrossRef]
16. Gope, P.; Hwang, T. BSN-Care: A Secure IoT-based Modern Healthcare System using Body Sensor Network. *IEEE Sens. J.* **2015**, *16*, 1368–1376. [CrossRef]
17. Alshahrani, M.; Traore, I. Secure Mutual Authentication and Automated Access Control for IoT Smart Home using Cumulative Keyed-hash chain. *J. Inf. Secur. Appl.* **2019**, *45*, 156–175. [CrossRef]
18. Dhillon, P.K.; Kalra, S. Multi-Factor User Authentication Scheme for IoT-based Healthcare Services. *J. Reliab. Intell. Environ.* **2018**, *4*, 141–160. [CrossRef]
19. Rani, S.S.; Alzubi, J.A.; Lakshmanaprabu, S.K.; Gupta, D.; Manikandan, R. Optimal Users based Secure Data Transmission on the Internet of Healthcare Things (IoHT) with Lightweight Block Ciphers. *Multimed. Tools Appl.* **2020**, *79*, 35405–35424. [CrossRef]
20. Alassaf, N.; Gutub, A.; Parah, S.A.; Al Ghamdi, M. Enhancing Speed of SIMON: A Light-Weight-Cryptographic Algorithm for IoT Applications. *Multimed. Tools Appl.* **2018**, *78*, 32633–32657. [CrossRef]
21. Han, S.; Gu, M.; Yang, B.; Lin, J.; Hong, H.; Kong, M. A Secure Trust-Based Key Distribution with Self-Healing for Internet of Things. *IEEE Access* **2019**, *7*, 114060–114076. [CrossRef]
22. Yeh, K.H. A Secure IoT-based Healthcare System with Body Sensor Networks. *IEEE Access* **2016**, *4*, 10288–10299. [CrossRef]
23. 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]
24. Rathee, G.; Sharma, A.; Saini, H.; Kumar, R.; Iqbal, R. A Hybrid Framework for Multimedia Data Processing in IoT-Healthcare using Block Chain Technology. *Multimed. Tools Appl.* **2019**, *79*, 9711–9733. [CrossRef]
25. Sharma, G.; Kalra, S. A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services. *Iran. J. Sci. Technol. Trans. Electr. Eng.* **2019**, *43*, 619–636. [CrossRef]
26. Ashraf, Z.; Mahmood, Z.; Iqbal, M. Lightweight Privacy-Preserving Remote User Authentication and Key Agreement Protocol for Next-Generation IoT-Based Smart Healthcare. *Future Internet* **2023**, *15*, 386. [CrossRef]
27. Shakeel, P.M.; Baskar, S.; Dhulipala, V.R.S.; Mishra, S.; Jaber, M.M. Maintaining Security and Privacy in Health care System using Learning based Deep-Q-networks. *J. Med. Syst.* **2018**, *42*, 186. [CrossRef]
28. Xu, K.; Li, Z.; Cui, A.; Geng, S.; Xiao, D.; Wang, X.; Wan, P. Q-Learning and Efficient Low-Quantity Charge Method for Nodes to Extend the Lifetime of Wireless Sensor Networks. *Electronics* **2023**, *12*, 4676. [CrossRef]
29. Nguyen, H.-S.; Danh, H.-C.; Ma, Q.-P.; Mesicek, J.; Hajnys, J.; Pagac, M.; Petru, J. A Bibliometrics Analysis of Medical In-ternet of Things for Modern Healthcare. *Electronics* **2023**, *12*, 4586. [CrossRef]
30. 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. [CrossRef]
31. Almaiah, M.A.; Yelisetti, S.; Arya, L.; Christopher, N.K.B.; Kaliappan, K.; Vellaisamy, P.; Hajjej, F.; Alkdour, T. A Novel Approach for Improving the Security of IoT–Medical Data Systems Using an Enhanced Dynamic Bayesian Network. *Electronics* **2023**, *12*, 4316. [CrossRef]
32. Vu, V.Q.; Tran, M.-Q.; Amer, M.; Khatiwada, M.; Ghoneim, S.S.M.; Elsisi, M. A Practical Hybrid IoT Architecture with Deep Learning Technique for Healthcare and Security Applications. *Information* **2023**, *14*, 379. [CrossRef]
33. Jagatheesaperumal, S.K.; Rajkumar, S.; Suresh, J.V.; Gumaei, A.H.; Alhakbani, N.; Uddin, M.Z.; Hassan, M.M. An IoT-Based Framework for Personalized Health Assessment and Recommendations Using Machine Learning. *Mathematics* **2023**, *11*, 2758. [CrossRef]
34. Irshad, R.R.; Hussain, S.; Sohail, S.S.; Zamani, A.S.; Madsen, D.Ø.; Alattab, A.A.; Ahmed, A.A.A.; Norain, K.A.A.; Alsaiari, O.A.S. A Novel IoT-Enabled Healthcare Monitoring Framework and Improved Grey Wolf Optimization Algorithm-Based Deep Convolution Neural Network Model for Early Diagnosis of Lung Cancer. *Sensors* **2023**, *23*, 2932. [CrossRef] [PubMed]
35. Kaliappan, V.K.; Gnanamurthy, S.; Yahya, A.; Samikannu, R.; Babar, M.; Qureshi, B.; Koubaa, A. Machine Learning Based Healthcare Service Dissemination Using Social Internet of Things and Cloud Architecture in Smart Cities. *Sustainability* **2023**, *15*, 5457. [CrossRef]
36. Peta, J.; Koppu, S. An IoT-Based Framework and Ensemble Optimized Deep Maxout Network Model for Breast Cancer Classification. *Electronics* **2022**, *11*, 4137. [CrossRef]
37. Lakshmanna, K.; Kaluri, R.; Gundluru, N.; Alzamil, Z.S.; Rajput, D.S.; Khan, A.A.; Haq, M.A.; Alhussen, A. A Review on Deep Learning Techniques for IoT Data. *Electronics* **2022**, *11*, 1604. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.