International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey on Deep Learning Based Techniques for Secured Prediction Model in Iot-Smart Healthcare Devices

S.Senthamarai[1] , Dr.R.Mala[2], Dr.V.Palanisamy[3]

[1]Research Scholar, Alagappa University, Karaikudi
[2]Assistant Professor, Department of CSE, Government College of Arts and Science College for Women, Paramakudi, Tamil Nadu
[3]Professor & Head, Department of Computer Applications, Alagappa University,Karaikudi – 630 004

ABSTRACT

Healthcare Devices connected to the Internet of Things (IoT) are being used more often by users to track their health and fitness progress. Despite the general public's growing embrace of healthcare technology, IoT smart healthcare devices depend on sensitive user data to work properly and according to user preferences. Healthcare applications are more likely than other IoT applications to compromise user privacy. Implementing security mechanisms like encrypted, authorization, security systems, network monitoring, and security protocols for IoT smart healthcare devices and their shortcomings is pointless. As a result, to properly safeguard the IoT ecosystem, current security techniques need to be improved. Over the last several years, deep learning (DL) has made significant strides, and machine intelligence has evolved from a lab curiosity to use equipment in several crucial applications. Intelligent IoT device monitoring offers a substantial defense against fresh or zero-day threats. DL are effective strategies for data exploration for discovering "normal" and "abnormal" actions based on how IoT systems and smart healthcare devices function in an IoT setting. As a result, DL methods are essential for transforming IoT security from only providing secure communication between devices to security-based intelligence systems. This study's goal is to give a comprehensive evaluation of DL methods and recent advancements that might be used to establish better security methods for IoT smart healthcare systems. The prospects, benefits, and drawbacks of each DL approach for IoT security are then presented after a comprehensive examination. We examine the advantages and drawbacks of using DL for IoT security. Finally, we assessed the performance rate for deep learning techniques in security prediction for smart healthcare devices. These possibilities and challenges might be used to guide the future study.

Keywords: Healthcare device, Internet of Things (IoT), Deep learning (DL), IoT security, security-based intelligence

INTRODUCTION

Connectivity advances, especially the Internet of Things (IoT), have facilitated significant development in environmental sensing practice in recent years. The information gathered, the data measured, and the understanding gained via the Internet of Things might pave the way for enhancements in the quality of life [1]. This circumstance makes it easier for people and other objects to communicate, which makes it possible to create smart cities. By the end of 2020, there will be 50 billion healthcare devices on the IoT, which is one of the computer science disciplines that are growing the fastest [2]. Existing technologies are crucial for enhancing real-world smart applications including home automation, the internet of vehicles, e-health, and e-education. On the other hand, IoT systems' huge scale, cross-cutting nature, and wide range of implementation-related components have led to new security concerns. IoT systems are complicated and feature integrated settings. In an IoT device with a huge attack surface, it is challenging to fulfill security needs. The whole information must be considered when developing solutions to meet the security need. IoT devices operate, however, mostly in unsupervised settings [3]. As a result, a burglar may get physical access to these gadgets. IoT smart healthcare devices are often linked through wireless networks, where a hacker might eavesdrop on a communication channel and acquire private data. IoT devices' low computational and power capabilities prevent them from supporting elaborate security mechanisms. Due to the IoT system's dual nature as a cyber-physical system component, its security architecture must account for not only constrained computational, conversation, and authority assets but also dependable engagement with the real world, especially in light of the latter's inherent instability. In the context of the Internet of Things, the autonomous nature of IoT smart healthcare systems necessitates that they continually adapt and thrive accurately and predictably, with safety as their top concern. The Internet of Things ecosystem also opens up new entry points for hackers. Such attack vectors are provided by the interconnected and contextual nature of the Internet of Things [4]. As a result, the security of IoT systems is in greater danger than that of other computer systems, and the conventional approach may not work for such systems. The widespread use of IoT has several consequences, including the fact that IoT implementation is now a linked process. IoT systems, for illustration, need to think about things including energy savings, safety, massive IoT data analytics methods, and program interoperability, all at once at the implementation phase. When thinking about advancements in one area, one cannot disregard the other [5]. Figure 1 shows how monitoring IoT devices may prevent zero-day attacks. Deep learning is a strong data exploration tool for learning 'normal' and 'abnormal' IoT component and device behavior. Each portion of the IoT system's input data may be gathered and analyzed to establish typical interaction patterns, discovering malicious activity early [6]. DL approaches may intelligently forecast future unknown assaults by learning from current instances. New attacks are generally mutations of prior attempts. IoT systems must migrate from allowing secure device connectivity to DL-enabled security-based intelligence for effective and secure solutions [7].

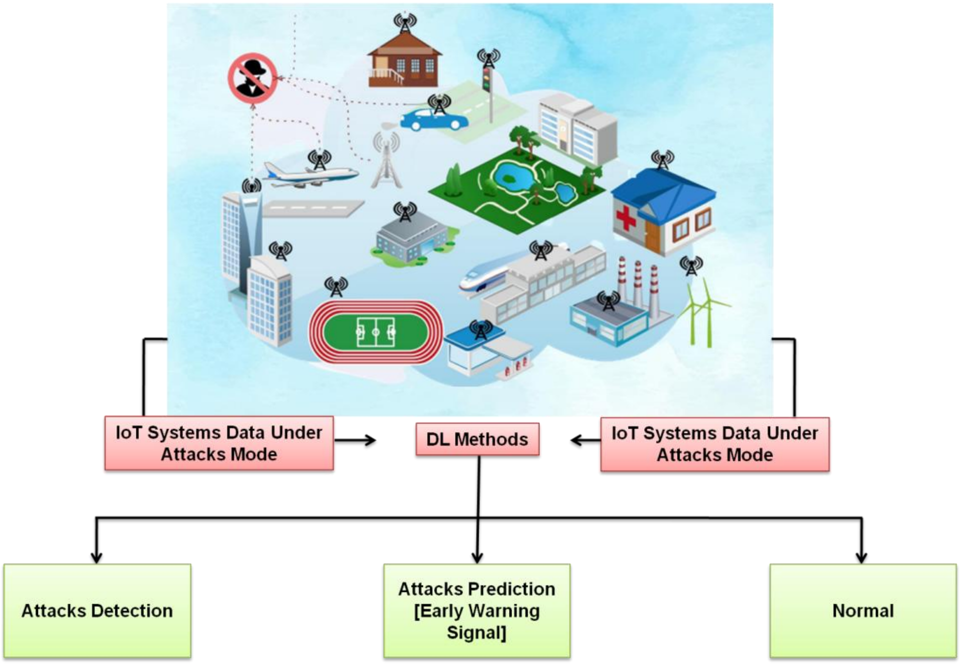
IoT Systems Data Under Attacks Mode
DL Methods
IoT Systems Data Under Attacks Mode
Attacks Detection
Attacks Prediction [Early Warning Signal]
Normal

Figure 1: DL in IoT security illustration

Researchers from diverse domains now have a new chance thanks to this integration to look at current IoT system difficulties from several angles [8]. However, since IoT devices are widely dispersed and have a vast and exposed surface, this integration also brings up new security difficulties. This feature of IoT devices creates several security concerns. Many valuable insights are also generated by the IoT platform. The insecure transfer and processing of this data might lead to major privacy breaches.

The further part of this paper is organized as follows: Part, II IoT security using Deep Learning (DL). Part III contains the performance evaluation. Part IV provides the conclusion.

IOT SECURITY USING DEEP LEARNING (DL)

The use of DL in IoT systems has recently become a crucial research area. The key benefit of using DL instead of classical machine learning is its higher performance on huge datasets. Many IoT devices generate a lot of data; as a result, DL approaches are appropriate for such systems. DL also can automatically extract sophisticated representations from data [9]. The IoT environment may be deeply linked using DL techniques [10]. IoT gadgets in a smart house, for instance, may automatically communicate with one another to create a complete smart home. Deep learning methods provide a multi-tiered computational framework for acquiring knowledge about abstracted data models (layers). Modern applications have been greatly improved by DL approaches compared to older ML methods [11]. The interpretation of signals by neurons and the cognitive domain has been used as a model for DL's development. Figure 2 indicates the Neural Networks (NNs) Working Principle for IoT Security Explained.

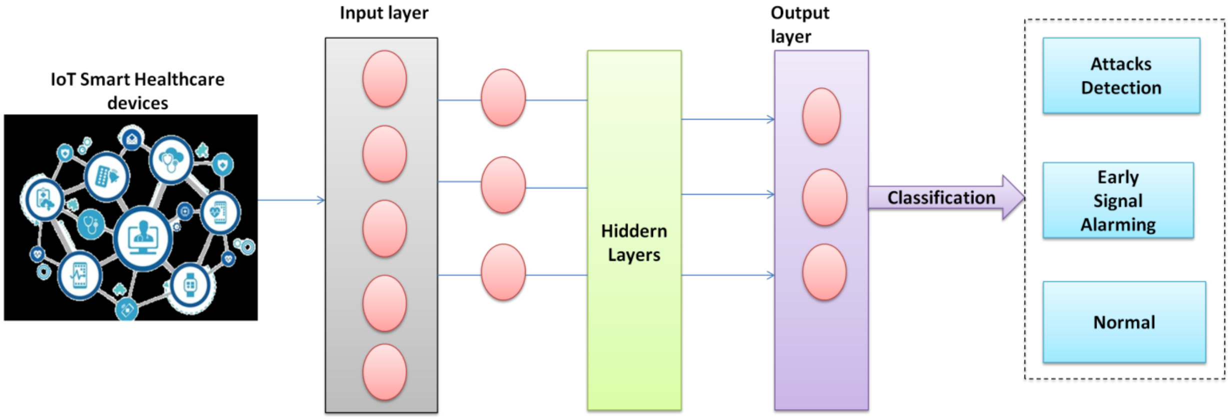

Figure 2: NNs Working Principle for IoT Security Explained

“Deep networks are built for supervised learning (discriminative learning), unsupervised learning (generative learning), and a mix of the two, known as hybrid DL. Discriminative DL approaches include CNNs and recurrent neural networks (RNNs). Hybrid DL approaches include Deep Belief Networks (DBNs), Restricted Boltzmann Machines (RBMs), Ensemble of DL Networks (EDLNs), Generative Adversarial Networks (GANs), and deep Autoencoders (AEs)”.

A. Convolutional Neural Network (CNN)

In contrast to traditional Artificial Neural Networks (ANNs), CNNs were designed to efficiently exploit much smaller datasets (ANN). We reduce the number of parameters by using three strategies: sparse interaction, parameter sharing, and suggested a strong representation. Keeping the number of connections between layers in a CNN increases its adaptability and decreases the difficulty of its training process. The CNN often alternates among convolutions and pooling layers. By using a succession of equal-sized filters (kernels), the convolutional layers incorporate the characteristics of the data [12]. To reduce the size of the succeeding layers, the pooling layers use average or maximum pooling. Additionally, a crucial layer is the activation unit of a CNN, which applies a non-linear encoder to each element of the feature set. Rectified Linear Unit (ReLU) activation function [13], utilized by nodes with the perceptron, is chosen to have a non-linear activation function $f(x) = max\ (0, x)$. One of CNN's greatest strengths is its widespread use as a teaching tool for DL. And what's more, it paves the way for fully automated, high-performance feature learning in the absence of any pre-existing models. However, the processing expense of a CNN makes it challenging to install it on healthcare devices with insufficient capabilities to support in-built security mechanisms. However, this issue may be solved by using a distributed architecture. Lightweight deep neural networks (DNNs) are developed and trained in this architecture by focusing on just a subset of the most important output classes, while the algorithm itself undergoes its full training on the cloud.

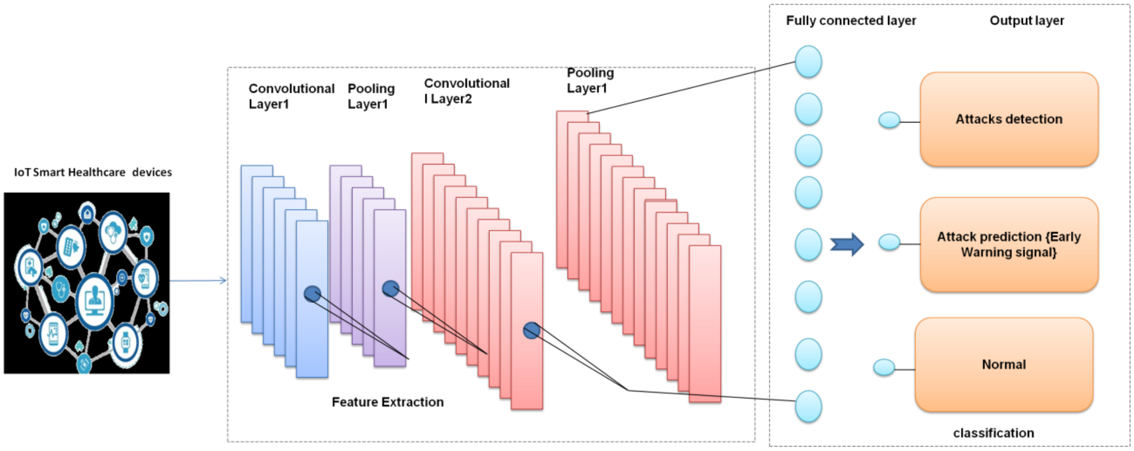

Figure 3: Sample of CNN's IoT Security Working Principle

Advances in image recognition are a primary motivation for CNN research and development. This widespread use of CNNs has allowed researchers to create very effective models for picture classification and identification by drawing on publicly available image databases like ImageNet. Using a CNN, the essential characteristics for malware detection may be automatically learned from the raw data, doing away with the requirement for labor-intensive feature engineering. In contrast to standard ML, which requires an extraction step before modeling can begin, a CNN is trained to learn appropriate features and conduct classification concurrently, resulting in an end-to-end model [14]. CNN has impressive learning performance, however, this may be exploited by malicious actors.

B. Recurrent Neural Network

For DL purposes, a Recurrent Neural Network (RNN) is a crucial kind of algorithm. The use of RNNs to process sequential data was suggested. The study of relationships from several prior samples is used in several applications to predict the present output. In this way, the neural network's output is contingent on both current and previous inputs. Since the connection between the input and output layers is maintained without dependence, a feed-forward NN is not suitable for this setup. Therefore, the training of RNNs has been the most notable use of the backpropagation method since its inception [15].

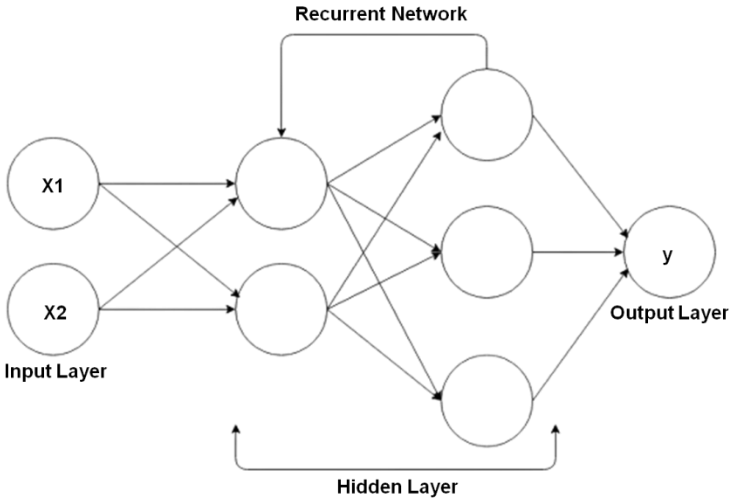

Figure 4: Architecture of RNN

RNNs use a temporal layer to collect sequential input, and then use the recurrent cell's covert hidden units to train to adapt to new environments. The input data is continually updated, and the concealed units are subsequently changed to represent the current condition of the network [16]. After analyzing the current hidden state, the RNN predicts the next hidden state as the result of activating the previous hidden state. To properly manage sequential data, RNNs are employed. This capacity is helpful in many contexts, including threat detection where analysis of threat trends across time is essential. As a result, recurrent connections are a powerful tool for training neural networks and uncovering hidden patterns of behavior. However, RNNs' fundamental problem is that they may experience disappearing or exploding gradients [17].

C. Restricted Boltzmann Machines (RBMs)

RBMs are unsupervised learning's deep generative models. To put it another way, RBM is a model in which there is no connection between any two nodes on the same layer [18]. In RBMs, there are both open and concealed layers. Layer one contains the known input, while layer two or more contain the latent variables. As a result of their hierarchical understanding of data features, In the second layer, RBMs may utilize the previous layer's collected characteristics as latent variables. Overcame the difficulties associated with creating a network anomaly detection model [19]. One of the challenges is labeling data in a network traffic dataset, which is multi-part and inconsistent so that it can be used to efficiently train a model. As a result, the second difficulty is that anomalous behavior is always changing. Consequently, the model needs to be flexible enough to identify novel forms of attacks and general enough to spot the outlier in a variety of network settings.

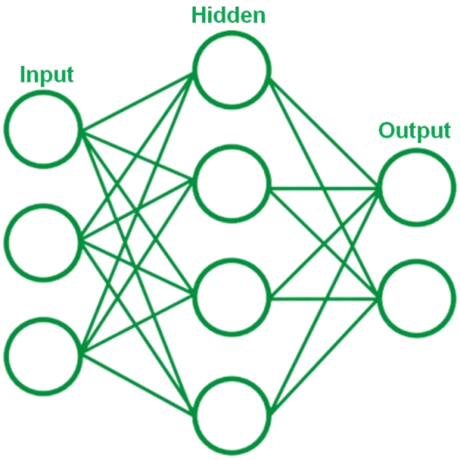

Figure 5: Structure of RBM

These problems are tackled head-on by the authors who provide a discriminative RBM-based learning model. This conclusion needs further research, as does the question of whether or not a classifier can be generalized to identify an abnormality across a variety of network settings [20]. A single RBM can only represent so many different features. On the other hand, a DBN can be created by stacking multiple RBMs together. The following section elaborates on this procedure.

D. Deep Belief Networks (DBNs)

DBNs have generated techniques that are constructed from layered RBM levels and trained greedily at each layer to achieve superior performance in an uncontrolled environment. DBNs are feed-forward networks for weight fine-tuning with metadiscourse resolution [21], transitioning from a pre-training phase consisting of a sequence of RBMs layers. Each successive layer is trained as if it were a separate RBM and learning signs of progress in this manner from beginning to end. In the pre-training stage, a selfish layer-wise unsupervised approach is employed to train the first characteristics; afterward, in the tuning phase, a softmax layer is applied to the top layer to fine-tune the characteristics concerning the classification techniques [22]. The detection of malicious attacks is one area where DBNs have been effectively deployed. In this work, a DBN was employed for automated detection, and compared to ML-based methods, the suggested DBN-based model significantly improved the accuracy with which malware was detected. This finding proved that DL, and DBNs in particular, are much better than conventional manual feature engineering techniques for detecting malware. Deep belief networks (DBNs) are unsupervised learning algorithms that are trained repeatedly to accurately represent features using unlabeled input. Despite DBNs' use of contrastive convergence to cut down on processing time, such networks are still not suitable for onboard devices due to their low resource requirements [23].

E. Generative Adversarial Networks (GANs)

In the last several years, GANs have become a potentially useful DL framework. As demonstrated in figure 6, a GAN framework uses an adversarial approach to train two models at once: a generative model and a discriminative model. By studying the distribution of data, generative models may produce new samples, whereas discriminative models can determine whether or not a sample was generated by the generative model or the training dataset [24]. Different from the generator, the discriminator is given multiple samples of the actual data from the training set. The goal of the discriminator is to separate training dataset actual samples from generative model fake ones. Samples that are successfully and erroneously labeled are used to evaluate the effectiveness of a model's discriminative and generative capabilities, respectively. Both models are then revised for the subsequent cycle. As a result, the discriminative model at the output aids the generative model in improving the quality of the samples it generates for the next cycle. Recently, GANs have been used to the problem of protecting the Internet of Things. For instance, the authors present an architecture for protecting the online presence of IoT devices, and a key part of this solution is the use of deep learning (DL) algorithms to determine if a device's behavior is typical or out of the ordinary [25].

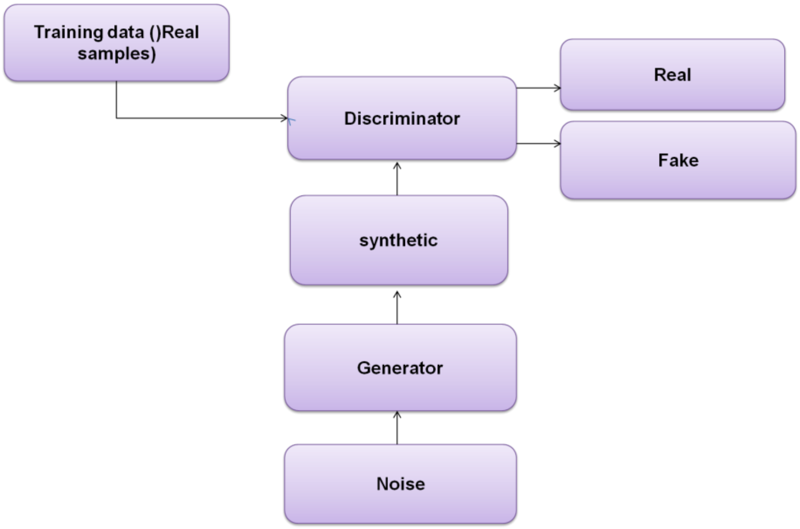

Figure 6: GAN Working Principle Illustration

Preliminary research included GAN algorithms in the suggested design, and assessment findings demonstrated the GAN-based architecture's efficacy in identifying anomalous system behavior. Because GANs may be trained to create samples that are comparable to a zero-day attack, and because they can offer algorithms with a collection of samples beyond the known assaults, they may have possible use in IoT security. In a semi-supervised setting, GANs excel in training classifiers. Since GANs don't need to produce unique sample entries sequentially, they can generate samples at a far faster pace than completely visible DBNs. Contrary to RBMs, which need an unknown number of Markov chain iterations to generate a sample, GANs only require a single model iteration to do so [25]. GAN training, however, is notoriously unreliable and challenging. Training a GAN to create discrete data, like text, is difficult.

F. Ensemble of DL networks (EDLNs)

Many DL algorithms can work together to outperform those that are performed alone. Combining generative, discriminative, or hybrid models is one way to create EDLNs. EDLNs are often used for dealing with challenges of great dimensionality and uncertainty [26]. To improve variety, accuracy, performance, and generalization, an EDLN stacks many individual classifiers. These classifiers may be homogeneous or heterogeneous. Despite the widespread success of EDLNs in areas like human activity recognition, their potential use in Internet of Things (IoT) security has yet to be fully explored [27]. More study into the use of lighter homogeneously or heterogeneously classifiers in a distributed setting is necessary to increase the accuracy and effectiveness of an IoT healthcare security system all while discussing issues posed by computation.

G. Deep Autoencoders (AE)

Deep AEs are a kind of artificial neural network (ANN) that can learn from data inputs without being given any outputs. Input data from users is handled by an AE's hidden layer (h), which assigns a unique value to each piece of input. For an AE neural network to operate, both the encoder's $h = f(x)$ and the decoder's r = g(input) functions must be in place (h). To create a code, an encoder must first abstract information from its original form [28]. Next, the decoder utilizes the code that was created to represent the input to recreate the original input [29]. The training process for AEs should produce as few reconstruction errors as feasible. The widely held idea that AEs can learn to provide identical output to input is false. Artificial emulations can only build a rough imitation by continually replicating training data. Because it must prioritize which input attributes to reproduce, the model learns meaningful facts. When looking for malware on a network, researchers turned to AEs, which had been taught to understand the latent representation of a wide variety of features.

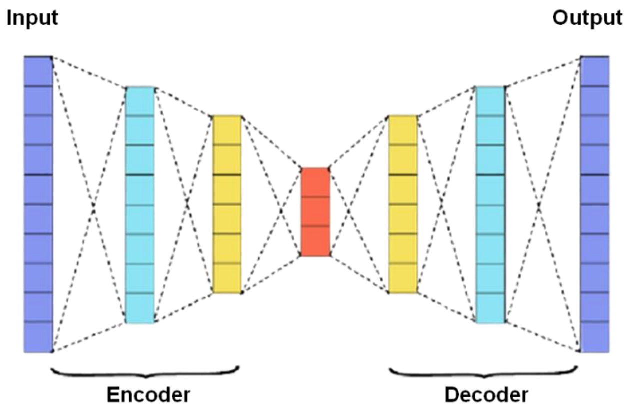

Figure 7: Architecture of AE

The AEs outperformed the standard ML algorithms SVM and KNN in terms of detection accuracy. In a different piece of research, an AE was used in tandem with a DBN to build a malware detection technique, with the AE performing non-linear mapping on the data to extract just the most relevant characteristics, and the DBN being taught to recognize dangerous code. Table 1 indicates the Potential DL techniques for IoT system security [30].

Table 1: Potential DL techniques for IoT system security

Techniques	Working principle	Merits	Demerits	Suggested Use for IoT Security
CNN	CNN's minimize the number of connections across layers by using encounters with few exchanged values, shared metrics, and depictions that are equivalent to all orientations.	CNN's are high-performing supervised DL algorithms. CNNs' scalability and training time complexity are addressed with additional features. CNN's can learn IoT security aspects from raw data.	CNNs are computationally expensive; It's challenging to implement them on low-powered devices for onboard protection.	The features of security data may be automatically learned by CNNs, allowing them to construct a full security model for Connected systems.
	RNNs collect sequential input and learn multi-faceted variations using the recurrent cell's hidden unit.	RNNs and their variations perform well with sequential data. In certain circumstances, IoT security data is sequential, therefore RNNs might be used.	RNNs' disappearing or bursting gradients are a problem.	RNNs can identify malicious network traffic with high accuracy. RNNs and their variations may improve IoT security, especially for time series-based attacks.
RBM	RBMs are unsupervised generative models. Undirected models have no links between same-layer nodes.	Using RBM feedback enables unsupervised extraction of several key characteristics.	For onboard security, it might be challenging to implement RBMs on asset IoT devices.	RBMs identify network anomalies.
DBN	DBNs use layered RBMs with greedy layer-wise training for unsupervised performance.	DBNs are trained repeatedly using unlabeled data for substantial feature representation.	DBNs have substantial computational costs owing to their complex initialization procedure.	DBNs can identify attacks.

GAN	The discriminative model predicts the sample source, whereas the generating model is a trained dataset and creates samples.	With DBNs and RBMs, GANs only need one model pass to create samples.	GAN training is unreliable. GAN data generation is tricky.	GANs can secure IoT cyberspace.
EDLN	EDLNs are multimodal, generating, and discrete.	Incorporating several DL classifications increases model variety, efficiency, and adaptability.	Increase system time complexity.	GANs are suggested for IoT security, especially for developing lightweight homogeneous and heterogeneous classifications in a dispersed scenario.
	AE	Encoders take data and convert it into machine-readable code. To recover the original signal, the decoder deciphers the input code.	AEs may replace manually designed features in classical ML and decrease dimensionality without previous data expertise.	AEs are quite processor-heavy. Instead of accurately representing the attributes of a dataset, AEs might add unnecessary complexity to the learning process.

PERFORMANCE EVALUATION

This study's goal is to give a comprehensive evaluation of DL methods and recent advancements that might be used to establish better security methods for IoT smart healthcare systems. After a thorough analysis, the possibilities, advantages, and disadvantages of each DL technique for IoT security are then provided. Finally, we evaluated the effectiveness of deep learning algorithms for healthcare smart device security predictions using accuracy, sensitivity, and specificity using methods such as CNN, RNN, RBM, DBN, GAN, EDLN and AE. Figure 8 indicates the performance rate of Deep learning algorithms. Table 2 indicates the Performance rate of DNN methods.

Table 2: Performance rate of DNN methods

Performance rate%			
DNN methods	**Accuracy**	**Specificity**	**Sensitivity**
CNN	91	81	80
RNN	93	83	82
RBM	94	85	84
DBN	95	86	85
GAN	97	87	83
EDLN	97	88	86
AE	98	89	87

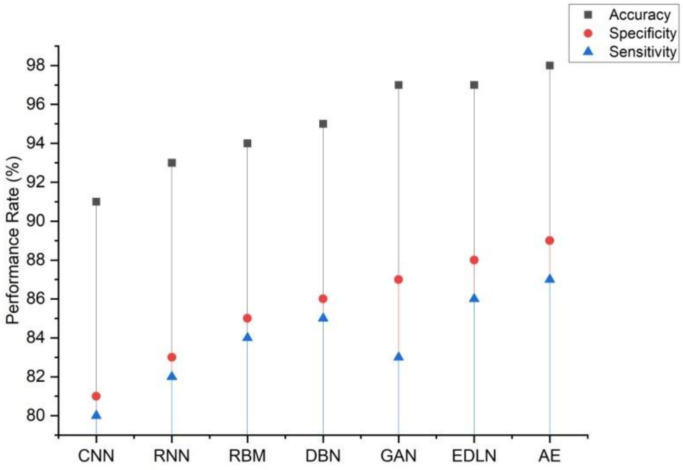

Figure 8: Performance rate of Deep learning algorithms

CONCLUSION

The requirements for protecting IoT devices have become more complicated as a result of the need to secure and integrate many technologies, from mobile and cloud architectures to physical devices and wireless transmission. Powerful analytical techniques that may be utilized to improve IoT security prediction in smart healthcare devices have been developed thanks to the development of DL. Various IoT security risks and IoT attack surfaces are included in this study. The possible applications of DL techniques in IoT security are thoroughly reviewed. The merits, drawbacks, and applications of these techniques are then contrasted after each subsection. The applications of DL approaches for safeguarding the primary IoT layers—namely, the perception, network, and application layers—are then discussed. We highlight issues, difficulties, and potential possibilities for using DL techniques to address security flaws. Data, learning methodologies, IoT contexts, intrinsic DL challenges, and chances to combine IoT systems are categorized using DL with other techniques, complexity of the algorithm challenges, and privacy vs. various trade-off requirements. By developing a smart end-to-end IoT security prediction system in smart healthcare device-based techniques rather than only providing safe communication among IoT components, this survey hopes to motivate academics to increase the security of IoT systems.

Reference

1. Rahaman, A., Islam, M.M., Islam, M.R., Sadi, M.S. and Nooruddin, S., 2019. Developing IoT Based Smart Health Monitoring Systems: A Review. *Rev. d'Intelligence Artif.*, *33*(6), pp.435-440.
2. Riley, A. and Nica, E., 2021. Internet of Things-based Smart Healthcare Systems and Wireless Biomedical Sensing Devices in Monitoring, Detection, and Prevention of COVID-19. American Journal of Medical Research, 8(2), pp.51-65.
3. Alshehri, F. and Muhammad, G., 2020. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. IEEE Access, 9, pp.3660-3678.
4. Jaiswal, K., Sobhanayak, S., Turuk, A.K., Bibhudatta, S.L., Mohanta, B.K. and Jena, D., 2018, July. An IoT-cloud-based smart healthcare monitoring system using a container-based virtual environment in an edge device. In 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR) (pp. 1-7). IEEE.
5. Machorro-Cano, I., Alor-Hernández, G., Paredes-Valverde, M.A., Ramos-Deonati, U., Sánchez-Cervantes, J.L. and Rodríguez-Mazahua, L., 2019. PISIoT: a machine learning and IoT-based smart health platform for overweight and obesity control. Applied Sciences, 9(15), p.3037.
6. Muneer, A., Fati, S.M. and Fuddah, S., 2020. Smart health monitoring system using IoT-based smart fitness mirror. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18(1), pp.317-331.
7. Brown, J., Cug, J. and Kolencik, J., 2020. Internet of Things-based Smart Healthcare Systems: Real-Time Patient-Generated Medical

Data from Networked Wearable Devices. American Journal of Medical Research, 7(1), pp.21-27.

8. Ahmed, I., Jeon, G. and Piccialli, F., 2021. A deep-learning-based smart healthcare system for patient discomfort detection at the edge of the Internet of things. IEEE Internet of Things Journal, 8(13), pp.10318-10326.
9. Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M. and Imran, M., 2020. Deep learning and big data technologies for IoT security. Computer Communications, 151, pp.495-517.
10. Li, W., Chai, Y., Khan, F., Jan, S.R.U., Verma, S., Menon, V.G. and Li, X., 2021. A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare systems. Mobile Networks and Applications, 26(1), pp.234-252.
11. Praveen, K.V., Prathap, P.J., Dhanasekaran, S., Punithavathi, I.H., Duraipandy, P., Pustokhina, I. and Pustokhin, D.A., 2021. Deep learning-based intelligent and sustainable smart healthcare application in cloud-centric IoT. Computers, Materials, and Continua, 66(2), pp.1987-2003.
12. Anand, A., Rani, S., Anand, D., Aljahdali, H.M. and Kerr, D., 2021. An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications. Sensors, 21(19), p.6346.
13. Vimal, S., Robinson, Y.H., Kadry, S., Long, H.V. and Nam, Y., 2021. IoT-based smart health monitoring with CNN using edge computing. Journal of Internet Technology, 22(1), pp.173-185.
14. Xu, L., Zhou, X., Tao, Y., Liu, L., Yu, X., and Kumar, N., 2021. Intelligent security performance prediction for IoT-enabled healthcare networks using an improved CNN. IEEE Transactions on Industrial Informatics, 18(3), pp.2063-2074.
15. Chandol, M.K., and Rao, M.K., 2021. Border Collie Cat Optimization for Intrusion Detection System in Healthcare IoT Network Using Deep Recurrent Neural Network. The Computer Journal.
16. Saheed, Y.K. and Arowolo, M.O., 2021. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access, 9, pp.161546-161554.
17. Bhatia, M. and Kumari, S., 2021. A novel iot-fog-cloud-based healthcare system for monitoring and preventing encephalitis. Cognitive Computation, pp.1-18.
18. Lakhan, A., Mohammed, M.A., Rashid, A.N., Kadry, S., Abdulkareem, K.H., Nedoma, J., Martinek, R. and Razzak, I., 2022. Restricted Boltzmann machine Assisted Secure Serverless Edge System for Internet of Medical Things. IEEE Journal of Biomedical and Health Informatics.
19. Elsaeidy, A., Munasinghe, K.S., Sharma, D. and Jamalipour, A., 2019. Intrusion detection in smart cities using Restricted Boltzmann Machines. Journal of Network and Computer Applications, 135, pp.76-83.
20. Peter Soosai Anandaraj, A., Gomathy, V., Amali Angel Punitha, A., Abitha Kumari, D., Sheeba Rani, S. and Sureshkumar, S., 2021. Internet of Medical Things (IoMT) Enabled Skin Lesion Detection and Classification Using Optimal Segmentation and Restricted Boltzmann Machines. In Cognitive Internet of Medical Things for Smart Healthcare (pp. 195-209). Springer, Cham.
21. Nguyen, G.N., Le Viet, N.H., Elhoseny, M., Shankar, K., Gupta, B.B. and Abd El-Latif, A.A., 2021. Secure blockchain-enabled Cyber-physical systems in healthcare using a deep belief network with the ResNet model. Journal of parallel and distributed computing, 153, pp.150-160.
22. Javeed, M., Gochoo, M., Jalal, A., and Kim, K., 2021. HF-SPHR: Hybrid features for sustainable physical healthcare pattern recognition using deep belief networks. Sustainability, 13(4), p.1699.
23. Venkatasubramanian, S., 2022. Ambulatory Monitoring of Maternal and Fetal using Deep Convolution Generative Adversarial Network for Smart Health Care IoT System. International Journal of Advanced Computer Science and Applications, 13(1).
24. Vaccari, I., Orani, V., Paglialonga, A., Cambiaso, E. and Mongelli, M., 2021. A generative adversarial network (GAN) technique for Internet of Medical Things data. Sensors, 21(11), p.3726.
25. Lupión, M., Polo-Rodríguez, A., Medina-Quero, J., Sanjuan, J.F. and Ortigosa, P.M., 2022. On the limits of Conditional Generative Adversarial Neural Networks to reconstruct the identification of inhabitants from IoT low-resolution thermal sensors. Expert Systems with Applications, 203, p.117356.
26. Pati, A., Parhi, M. and Pattanayak, B.K., 2022. HeartFog: Fog Computing Enabled Ensemble Deep Learning Framework for Automatic Heart Disease Diagnosis. In Intelligent and Cloud Computing (pp. 39-53). Springer, Singapore.
27. Kumar, I.P., Mahaveerakannan, R., Kumar, K.P., Basu, I., Kumar, T.C.A. and Choche, M., 2022, March. A Design of Disease Diagnosis based Smart Healthcare Model using Deep Learning Technique. In 2022 International Conference on Electronics and Renewable Systems (ICEARS) (pp. 1444-1449). IEEE.

28. Ramachandran Manikandan, I., de Albuquerque, V.H.C., Tiwari, P., AlQahtani, S.A. and Hossain, M.S., Quality of Service-Aware Resource Selection in Healthcare IoT Using Deep Autoencoder Neural Networks.
29. Alo, U.R., Nweke, H.F., Teh, Y.W. and Murtaza, G., 2020. Smartphone motion sensor-based complex human activity identification using deep stacked autoencoder algorithm for the enhanced smart healthcare system. *Sensors*, *20*(21), p.6300.
30. Rajan Jeyaraj, P. and Nadar, E.R.S., 2020. RETRACTED: Atrial fibrillation classification using deep learning algorithm in the Internet of Things–based smart healthcare system. Health informatics journal, 26(3), pp.1827-1840.