Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 3642- 3656
Research Article

A Review on Deep Learning and Intrusion Detection System Technologies to Secure IoT

V. Surya[1], Dr. M. Muthuselvam[2]

[1]Research Scholar, Department of Computer Science, VISTAS, Pallavaram, Chennai.
[2]Assistant Professor of Information Tech., VISTAS, Pallavaram, Chennai .
Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract
Today the usage of internet has increased and the emergence of new technologies has invaded computer systems and networks. IoT is a new technology which opens up opportunities for new services and new innovations that is enabled by the developments in RFID, smart sensors and communication technologies. The fundamental aspect is to have smart sensors that communicate directly without human intervention to deliver a new application. All objects will be connected and are able to communicate with each other, while they operate in unprotected environments. This aspect leads to major security challenges. Companies are increasingly investing in these areas of research to optimize the detection of these attacks. Intrusion Detection Systems (IDS) are a vital tool for the protection of networks and data. Insights derived from the raw IoT data is highly complex that goes beyond the competence of traditional data analytical paradigms. Deep Learning models are better than conventional machine learning paradigms in the following ways. First, they mitigate the requirement for supervised feature sets to be utilized for training so that the features that might not be recognizable to a human can be extracted smoothly by Deep Learning models. This work focuses on the review related to IoT, IDS and Deep learning, traversing different areas related to security issues in IoT domain.

Keywords : Internet of Things, Intrusion detection System, Deep learning, Machine Learning, Security.

1. Introduction

IoT turns out to be the latest technology where devices are connected to one another and exchange information across the Internet. It is expected by 2022, billions of IP addresses or devices will be associated to the Internet through IoT networks.

More recently, IoT has been used to create smart surroundings, such as smart homes,smart traffic signs, smart parking spaces with a variety of system domains and related services. The main aim is to develop intelligent environments to make human life more productive and meaningful by addressing challenges related to housing, energy use, and industry needs. For example, Padova Smart City in Italy is a successful example of a smart city based on the IoT system [19].

The smart environment may contain sensors that act together to execute tasks. Wireless communication devices and IPv6 help expand smart areas. Such areas are vast, ranging from smart cities to health and intelligent services. The combination of IoT systems with intelligent environments makes smart things work better. However, IoT systems are affected by various security attacks such as denial-of-service (DoS) attacks and denial (DDoS) attacks. These types of attacks are very harmful and affects the services of IoT . So, security has become a major issue in IoT systems.

The intrusion detection system (IDS) is a software application system that detects the threats and alerts about the unusual behavior of the system. It acts in the network layer of the IoT system. The IDS embedded in the IoT system should be capable of examining data packets and produce real-time responses and check packets across different parts of the IoT network with diverse protocols, and get adjusted to various technologies in the IoT environment. IDS developed for intelligent IoT environments should operate under stringent conditions of fast response time, short processing power, and large volume data processing. Hence, standard IDS are not suitable to IoT environments. IoT security is therefore an ongoing and critical issue, which has to be dealt with the modern understanding of the security risks of IoT systems.

Also, machine learning techniques to detect intrusion into IoT is growing at a faster rate. Nevertheless, AI machine learning techniques often present low precision and are unable to detect attacks on large IoT networks. This work aims to investigate in-depth learning models of IoT entry-level acquisition.

Deep learning (DL) has powerful analytic capabilities that are used in various areas such as speech recognition, computer vision, medical diagnosis and bioinformatics. DL techniques shows a significant improvement in the performance than ML algorithms and is implemented in computer / fog applications. These applications require a large amount of information to be transmitted across the network, and DL provides better performance with wider data than ML. Alternatively, DL can use new features to solve problems and arrive at a better solution without human intervention.

Technologies are emerging everyday and changes are coming up. The development of the 5G network plays a vital role in IoT systems and services. 5G network catches the attention of the investigators and generates inquisitiveness about the probable security and privacy risks. Therefore, it is essential to understand the risk factors of security and potential solutions.

The effort put in this work is to promote the development of an in-depth IDS framework (DL-IDS) to protect IoT sites through effective detection of attacks.

2. Review of Literature

AL-Hawawreh et al, [11] proposed an anomaly detection system(ADS) for Internet Industrial Control Systems (IICSs) centered on deep learning techniques which learns and authenticates data collected from TCP/IP packets. The ADS is executed using the deep auto-encoder and deep feed forward neural network architecture and tested with training data sets namely NSL-KDD and UNSW-NB15. The author has compared the ADS model designed with the other recently developed techniques viz. the Filter-based Support Vector Machine (F-SVM), Computer Vision Technique (CVT), Dirichlet Mixture Model (DMM), Triangle Area Near- est Neighbors (TANN), DBN, RNN, DNN, and Ensemble-DNN. All these models are tested on NSL- KDD dataset in term of detection rate and false positive rate. The author has achieved the best results with 99% DR and 1.8% FPR. Since the experimental results shows that the ADS technique can achieve a higher detection rate and lower false positive rate, it could be used in intrusion detection system in IoT.

da Costa et al, [1] focuses mainly on machine learning algorithms applied to Internet of Things to detect intrusion and enhance network security. More than 95 works were surveyed in this paper related to IoT and its security.

This paper presents relevant works emphasizing on IoT using many intelligent intrusion detection techniques to ensure network security.

Mardiana binti Mohamad Noor and Wan Haslina Hassan [13] planned the work in IoT security with the aid of the available simulation tools, modelers, and computational and analysis platforms. The author has actually presented an analysis of recent trends and open issues in IoT security from 2016 to 2018. This paper mainly provides an overview of the recent development of IoT security.

Mohamed Faisal Elrawy et al,[5] article presents a broad analysis of the latest IDSs designed for the IoT model, featuring the methods and implementation. This article discusses deeply the IoT architecture, security hazard issues relative to the layers of the IoT architecture. The author

besides demonstrating the design and implementation of IDSs for the IoT paradigm, has explained clearly how crucial it is to develop an efficient, reliable and robust IDSs for IoT-based smart environments. The development of efficient IDSs forms the future study of the survey.

Suchitra.C and Vandana C.P [16] has explored the recent trend of internet of things and analyzed the various security issues and their limitations in each layer of IoT. Securiy in IoT is the need of the hour and this paper has analyzed the various security requirements and challenges in IoT and the objectives of research.

Tausifa Jan Saleem and Mohammad Ahsan Chishti [9] presents how deep learning is effective in analyzing the complex data generated by IoT applications. Further the author has discussed about the various deep neural network architectures namely Restricted Boltzmann Machine , Deep Belief Networks,Convolutional Neural Network, Recurrent Neural Network , Long Short Term Memory, Auto-Encoders and Generative Adversarial Networks and how these models are better than conventional machine learning models. Deep learning models for IoT use cases were explored and found that it is very much efficient for data analytics.

Ahanger et al [14] presented the importance of security in IoT. With the advancement of 5G network and the efficiency of IoT network, several security threats and their challenges are the main study in this paper.The solutions to tackle these issues are discussed. The applications of IoT and security threats concerning confidentiality,Availability,Authentiicty,Integrity and Non-repudiation are clearly discussed. Through this study it is made very clear that IoT wires several technologies and services. IoT is not a single application platform. On the whole, the researcher has provided various issues related to security and privacy at all architectural levels for successful functioning of IoT.

Ge et al [12] used a new data set called Bot-IoT for intrusion detection scheme for IoT networks using deep learning concepts. The authors have proposed a framework for IDS in IoT networks. The framework has four phases namely feature extraction, feature preprocessing, training and classification. A feed-forward neural network(FNN) model for binary and multi-class classification is developed which includes denial of service, distributed denial of service and information theft attacks against IoT devices.The FNN model is compared with Support Vector Classifier(SVC) model for multiclass classification and found that that FNN is efficient and obtained high accuracy for large dataset.

Otoum et al ,[10] proposed a new deep learning algorithm based intrusion detection system (DL-IDS) to identify threats in IoT and to secure the environment. Many traditional IDS have already been dealt in the literature, but they lack optimal features learning and data set management, which affect the accuracy of attack detection. The proposed model uses spider monkey optimization (SMO) algorithm to select the optimal features in the data set. Also the stacked-deep polynomial network (SDPN) model is used which classifies whether the data set is normal or abnormal. The attacks detected by DL-IDS include denial of service (DoS), user-to-root (U2R) attack, probe attack, and remote-to-local (R2L) attack. The authors have evaluated the DL-IDS system using the NSL-KDD data set and the performance metrics such as accuracy, precision, recall, and F score are found to be excellent.

In the same context Geethapriya Thamilarasu and Shiven Chawla [6], presented an intelligent intrusion-detection system to identify threats in the inseure IoT network. As deep learning techniques outperform machine learning algorithms in detecting attacks and producing good accuracy measures, DL is used to detect anomalous behavior in IoT. The authors have tested their DL based IDS performance against five different attacks namely black hole attack, opportunistic service attack, DDoS attack, sinkhole, and wormhole attacks. The performance of the detection system is evaluated using the metrics recall, precision, and F1 score. The

framework is tested in both real network set up and using simulation. The experimental result confirms that the detection system is robust and is able to detect various network attacks.
Tawalbeh et al[8] , With the main concern on security and privacy issue the authors have presented a new generic and stretched IoT layered model. The generic and stretched model is as shown in the figure 1:

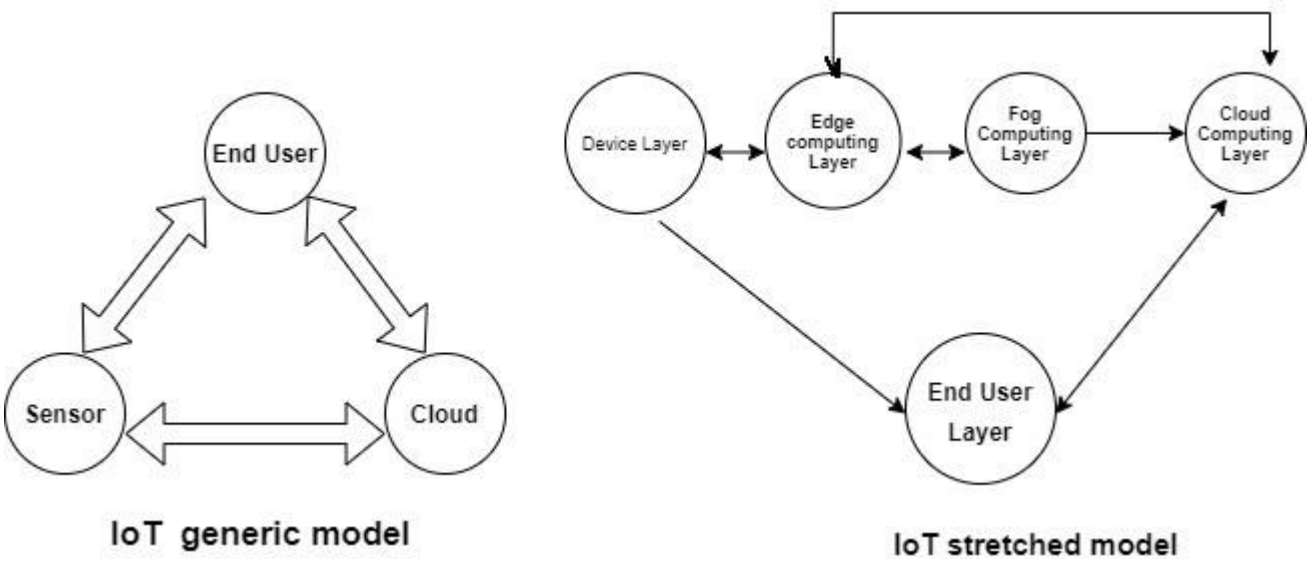

Figure 1. IoT – Generic and Stretched model

The IoT model proposed by the author is supported by cloud and edge computing. It is implemented and the performance is evaluated successfully. The cloud-edge IoT layered model is shown in figure 2. It is a three layered architecture.

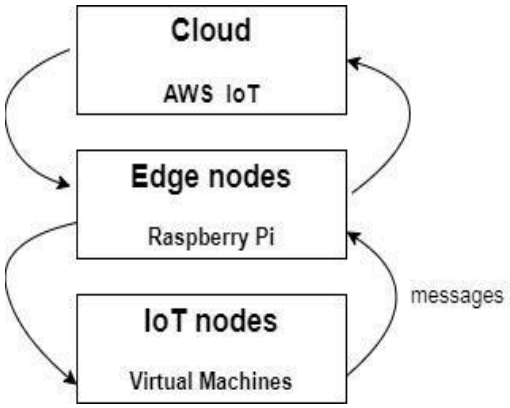

Figure 2. Cloud Edge Layered IoT model

- The lower layer represents the IoT nodes as Virtual Machines generated by the Amazon Web Service (AWS).
- The middle layer serves as a edge and it is implemented as a Raspberry Pi 4 hardware kitwith support of the Greengrass Edge Environment in AWS.
- The top layer represents the cloud-enabled IoT environment.

The security protocols between the layers were used to protect the users information ensuring privacy. The new model is designed with the best security measures and is efficient in handling cyber threats at each of the above layers namely cloud,edge and IoT.
Mohamed Abomhara and Geir M. Koien [17], discussed on the tremendous growth of IoT, IoT architectures, supporting technologies and the existing security threats in IoT. A wide discussion on IoT security requirements and future research directions are presented. This paper gives immense information on the current status and provides open issues and challenges in IoT domain.
Aldowah et al [15], the authors reviewed the research progress of IoT and secured new solutions for several security issues from Academicians, Technicians and Industry experts . This paper provides the solutions that need to be developed and deployed to provide confidentiality and integrity in heterogeneous environment.
Shafique et al [7] presents an elaborate view of the upcoming fifth generation IoT scenario. Fifth Generation (5G) cellular networks use the latest technologies namely carrier aggregation, multiple-input multiple output (MIMO), massive-MIMO (M-MIMO), coordinated multipoint processing (CoMP), device-to-device (D2D)

communications, centralized radio access network (CRAN), software-defined wireless sensor networking (SD-WSN), network function virtualization (NFV) and cognitive radios (CRs). This paper gives a clear review of these key enabling technologies and also presents the new use cases of 5G-IoT. Ultimately the paper provides the challenges of 5G-IoT in both cloud-based platforms and IoT devices based edge computing.

3. Taxonomy of the Literature Review

A taxonomy of Literature reviews in the broad area of IoT with the prime focus on security is as shown in figure 3.

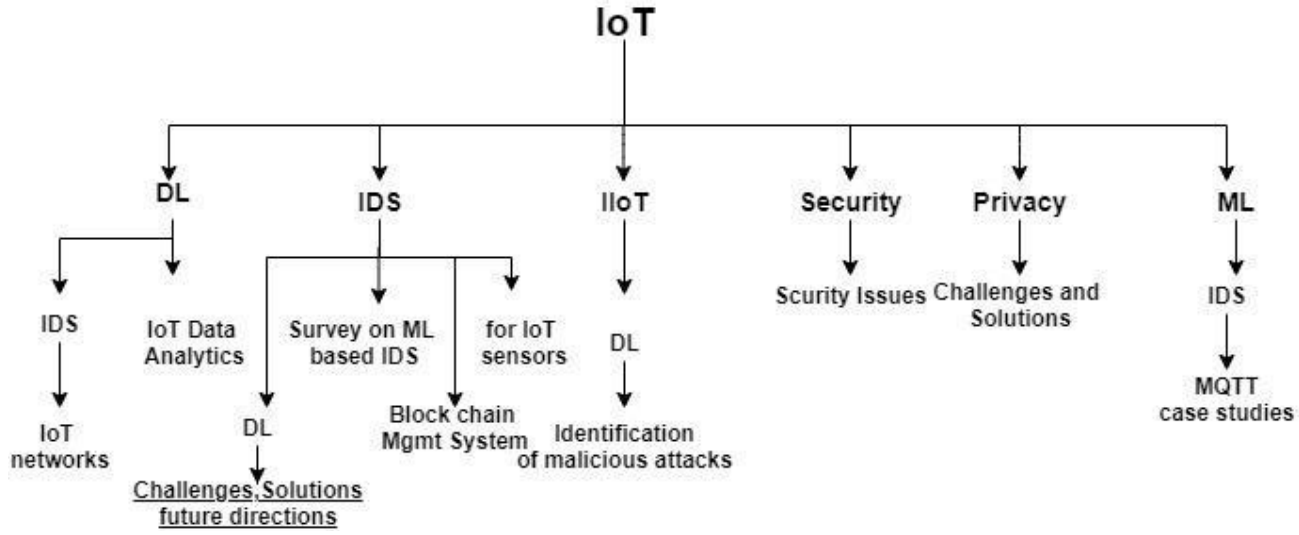

Figure 3. Taxonomy of Literature Reviews

4. Data sets and Methodology

The widely used data set and the methodology employed in different works of this paper related to IoT and security are presented here.

Diro and Chilamkurti [2] performed experiments using three different datasets namely KDDCUP99, ISCX, and NSL-KDD to detect intrusion in computer networks. To detect the attacks they have put forward, a distributed deep learning-based IoT network system. The outcome of the experimental results shows the appropriate usage of artificial intelligence techniques for network security. The performance is measured in terms of accuracy, detection rate, and false alarm rate and it has shown the effectiveness of deep models over shallow models.

It is found that , most of the datasets used for research are commonly used by other researchers for their work. In essence, it is found that a lot of research proposed uses more classifiers with different datasets and analyzed the performance based on the metrics such as accuracy, error rate, and primarily the feasibility to employ in IoT devices.

Guo et al. [3] carried out an interesting work on IoT-based applications on smart cities such as traffic control, unattended vehicle parking, tracking the company's assets and monitoring, geolocation. The authors had developed a framework using Adaboost and Random forest classifiers for this IoT based applications. Convolutional Neural Networks(CNN) have an excellent image classification tasks and the recent studies shows that it can be applied to IoT devices, especially when the data set is large.

Shen et al. [4] employed CNN on IoT applications to sharpen on the high requirement for communication and data training. For training and testing , two popular datasets, MNIST and CIFAR-10, were used. The MNIST dataset contains 60,000 training examples and 10,000 for testing purposes. The CIFAR-10 dataset consists of 50,000 training examples and 10,000 for testing. The digital image size is 28 ×28. On implementing it on IoT devices, it is found that the results were promising and appropriate to achieve good performance

Some of the datasets used in the works of this paper are summarized in Table 1 below :

Table 1: Datasets used

Data set	Size	Type of the dataset
KDD '99,Noisy dataset	-	Raw data
NSL-KDD	-	Symbolic data
NSL-KDD	148,517	Text file
NSL-KDD	148,516	
KDD CUP 1999	212,123 samples	-
KDD	148,753 records	
MNIST, CIFA-10	70,000, 60,000	Image data
Open dataset from Kaggle	25000	Image Data
KDD99	548,015	Network data

5. Open Issues

IoT applications are tremendously growing and at the same time security has become a threat. To overcome the potential threat, lots of work are to be developed to increase the reliability in IoT applications. Therefore, the trend is now to focus on the security challenges in IoT services and devices.

IoT is combined with big data and multiple technologies, hence challenges in security has become a prime issue. Also , there is a limitation on the availability of services for IoT, hardware limitations for applications, access to remote locations and so on.These limitations are specifically addresses and are being explored.

The literature also focused on the use of Intrusion detection system tools to enhance security in IoT.

6. Conclusion

Based on the literature reviewed, it is found that the intrusion detection in IoT appears to be a challenge. Thus a highly challenging DL-IDS framework for IoT to detect severe anomalies with different classifiers can be employed and analyzed.

Moreover the emerging 5G-IoT technologies can be deployed in cloud and edge computing in IoT environment. The security issues, challenges and solutions are explored in depth in the survey on IoT, which is helpful for academicians, technical and industrial experts.

References

1. Kelton A.P. da Costa, João P. Papa, Celso O. Lisboa, Roberto Munoz, Victor Hugo C. de Albuquerque. "Internet of Things: A survey on machine learning-based intrusion detection approaches", Computer Networks, 2019 Publication
2. A .A . Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for internet of things, Future Gener. Comput. Syst. 82 (2018) 761–768 . [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S0167739X17308488
3. X. Guo, N. Ansari, L. Li, H. Li, Indoor localization by fusing a group of finger- prints based on random forests, IEEE Internet of Things Journal (2018) 1 . [On- line]. Available: doi: 10.1109/jiot.2018.2810601.
4. Y. Shen, T. Han, Q. Yang, X. Yang, Y. Wang, F. Li, H. Wen, CS-CNN: enabling robust and efficient convolutional neural networks inference for internet-of- things applications, IEEE Access 6 (2018) 13439–13448 . [Online].Available: doi: 10.1109/access.2018.2810264 .
5. Mohamed Faisal Elrawy1,2, Ali Ismail Awad3,4 and Hesham F. A. Hamed5 -Springer –Open Access (2018) - Intrusion detection systems for IoT-based smart environments: a survey
6. Geethapriya Thamilarasu * and Shiven Chawla 2019 Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things.
7. Challenges and Solutions. Kinza shafique 1, Bilal A. Khawaja 2,3, (senior member, IEEE), Farah Sabir4, Sameer Qazi 4, (member, IEEE), and Muhammad mustaqim –IEEE 2020-internet of things IoT) for next-generation smart systems: A Review of Future Trends and Prospects for Emerging 5G-IoT Scenarios
8. Lo'ai Tawalbeh 1,*, Fadi Muheidat 2 , Mais Tawalbeh 3 and Muhannad Quwaider 3 – 2020 IoT Privacy and Security: Challenges and Solutions.
9. Tausifa Jan Saleem, Mohammad Ahsan Chishti. "Deep Learning for Internet of Things Data Analytics", Procedia Computer Science, 2019 Publication.
10. Yazan Otoum1 Dandan Liu2 Amiya Nayak1-2019 DL-IDS: a deep learning–based intrusion detection framework for securing IoT
11. Muna AL-Hawawreh, Nour Moustafa, Elena Sitnikova. "Identification of malicious activities in industrial internet of things based on deep learning models", Journal of Information Security and Applications, 2018 Publication.
12. Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly(2019) IEEE- Deep Learning-based Intrusion Detection for IoT Networks
13. Mardiana binti Mohamad Noor , Wan Haslina Hassan-(2018) Current research on Internet of Things (IoT) security: A survey
14. Tariq Ahamed Ahanger, Abdullah Aljumah. "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms", IEEE Access, 2019 Publication.

15. Hanan Aldowah1(&), Shafiq Ul Rehman2, and Irfan Umar1Security in Internet of Things: Issues
16. Suchitra.C, Vandana C.P- IJCSMC, Vol. 5, Issue. 1, January 2016, pg.133 - 139 Internet of Things and Security Issues
17. Mohamed Abomhara, Geir M. Køien-2020 Security and Privacy in the Internet of Things:Current Status and Open Issues
18. Sweta Dave, Prof. Sandip Chauhan. "Intrusion Detection and Prevention System in IoT Environment", International Journal of Research in Advent Technology, 2019 Publication.
19. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
20. King J, Awad AI (2016) A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) 40(1):133–143
21. Weber M, Boban M (2016) Security challenges of the internet of things. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija. pp 638–643
22. Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Vienna. pp 84–90
23. Kafle VP, Fukushima Y, Harai H (2016) Internet of things standardization in ITU and prospective networking technologies. IEEE Commun Mag 54(9):43–49
24. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
25. Li H, OtaK,DongM. Learning IoT in edge: deep learning for the Internet of Things with edge computing. IEEENetwork. 2018;32(1):96-101.
