A survey on Deep Learning Methodologies for Internet of Things (IoT) Security

Akansha Bhargava[1], Gauri Salunkhe[2] and Prerna Goswami[3]

[123]Department of General Engineering, Institute of Chemical Technology, Matunga, Mumbai, India[1]minidimi@gmail.com, [2]gauri.2734@gmail.com, [3]p.goswami@ictmumbai.edu.in

Abstract

Internet of things is the term coined for all the devices that are connected and can exchange data. With the advent in technology, growth of the IOT industry has become extensive. IOT universe has made it possible for users to remotely monitor their network connected devices. However, IoT systems comprising Wireless Sensor Networks (WSNs), Radio Frequency Identifications (RFIDs), and cloud computing are exposed to numerous data privacy and security threats including intrusions, Denial of Service (DoS) attacks, spoofing attacks, Distributed Denial of Service (DDoS) attacks, malwares, jamming, eavesdropping amongst others[7].The larger number of the present day security solutions proliferate heavy computation and communication load for IoT devices, Most of the outdoor nodes and devices do not have high security protocols which make them highly susceptible to attacks. The review focuses on providing solution by implementing deep learning techniques to tackle the discussed issues.

Keywords: *IoT security, deep learning, attacks*

1. Introduction

IoT and cloud computing are being increasingly developed and deployed in various domains. Many IOT devices are personal to the individuals requiring high security and cannot afford to get compromised. For instance, in the healthcare domain to optimize patient safety, and operational efficiency the need for more secure infrastructure to protect data privacy has become a priority. However, the integration of IoT in the medical industry brings several challenges, including data storage, exchange of data between devices, security and privacy, and unified and ubiquitous access.

Another issue with having IOT devices is to schedule burgeoning mobile network traffic. This ever growing traffic needs to be scheduled in real time and should be reliable.

This review gives an insight on how deep learning methodologies can be implemented for detecting the attacks on IoT devices and about the various attacks associated with the different layers of IoT networks. An IoT system is shown in figure 1. The paper is collocated as follows:

- Compendious analysis of various threats and attacks in the IoT systems layerwise.
- Overview of DL methods, algorithms and applications for securing IoT systems.

ISSN: 2233-7857 IJFGCN

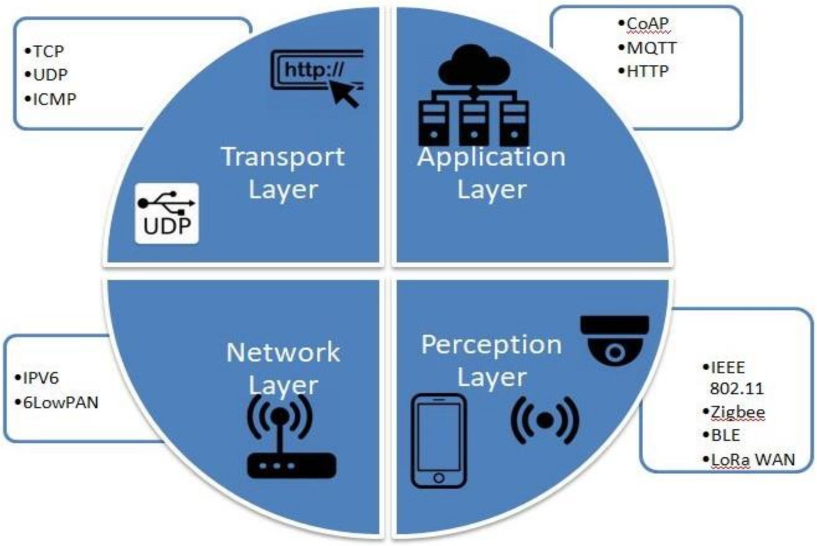

Figure 1. IoT System

2. Related Work

IoT networks are heterogeneous in nature and are speculated that for massive scale deployment of IoT devices existing internet will not suffice, which will also hinder the adaptability of advanced security solutions [1]. Authentication and authorization, privacy, end data security and trust among different devices of IoT are few open issues related to IOT security [2].

Security risks can be classified into cyber and physical attacks [3] potential methods for securing IOT using machine learning are required. Embedded security framework and architecture for lightweight security protocol that secure the operating system have been suggested in [4]. An algorithm has been developed and evaluated for Internet Protocol IPV6 and Low Power Wireless Personal Area Networks (6LoWPAN) security that provides end-to-end security for IoT using IPSec technology [5].Distributed and centralized division of IoT architecture makes it more challenging to implement security methods [6].An architecture with three platforms is proposed in [7] to tackle various challenges of unclear architecture and no specific standards.

Three types of interloper namely individual, organization and intelligence agencies are identified and a survey is done on how to tackle the issues related to security challenges [8].Machine Learning and Deep Learning techniques can provide the solution for various IoT threats and that can bridge the gap between existing threats and solutions [9].Aspects of Deep Learning are inspected to incorporate them to challenges introduced by big data analytics[10]. Edge computing can help in providing solutions for IoT security by moving service from cloud to edge network [11]. Cloud and Fog computing can be deployed to identify a malware and concurrently restraining it [12]. IOT systems generate large dataset and traditional machine learning approach doesn't fully give the security needed whereas deep learning methods prove to be superior when dealing with the large dataset. These algorithms are able to emulate the human brain’s capability to perceive, discern, assimilate, and incorporate decision, especially for extremely complex problems. Different DL algorithms are discussed that can be useful for providing higher security[3]. DL and ML require tremendous data and resources like memory, computation and energy, which are limited in case of IoT devices, hence deployment of DL becomes challenging [13]. IoT security needs to be characterized according to the IoT environment [14].

3. Security Challenges and Threats in IoT Deployment

Two major concerns for the IoT network are security and privacy. IoT makes it possible for physical devices to interact amongst each other and with the surroundings and usually these surroundings are heterogeneous in nature. Hence, the need for a comprehensive security of both the physical device and network is required [28]. However, the diversity of IoT systems creates more challenging and complex security needs.

The IoT device not only poses threat in the application domain but also for the device itself. These issues have been time and again discussed in various perspectives of attack environments e.g. communication, data, malware, cyber and physical attacks [34]. In essence, the extensive deployment of IoT devices over the last decade has also increased the attack surface and as most of these devices have limited resources employing sophisticated techniques to mitigate the attack becomes strenuous. IoT devices use different modes of communications such as IPV6, 6LowPAN, Bluetooth Low Energy, Long Range Wide Area Network and many more and these technologies have their own limitations. Broadly these threats can be classified as cyber and physical [3].

In physical attacks, the attacker pulverizes the sensors and end nodes thereby, completely hindering the operation. Although, these attacks can be unintentional also as IoT nodes are expected to be anywhere and everywhere in the external world so sometimes natural calamities can also affect the working [24]. Cyber attacks can be divided as active and passive.

Passive attacks are employed by listening to the communication channels and stealing the information over the network. In these kinds of attacks sensors are read and personal or valuable information can be collected which is a threat to privacy.

Active attacks include obstructing,disarranging and modifying the information of the system. The intruders eavesdrop the system and have the capability to take full control of it and impede the services of IoT devices. An attacker can inject a malware,impersonate or can manipulate the information. In any such situation, data can be altered affecting the proper functioning of a system.

The attack detection based on DL methods can take two approaches either by rule or by behavioral based [25]. Rule based techniques are superior when attacks are extensions of already existing attacks. It becomes challenging when the attacks are unique. So, the behavioral approach is being used which can easily detect new or unique attacks as it looks for anomalous behavior in the system so for any abnormal behavior will be tagged as an attack[26].A summary of various DL methodologies and attacks have been listed in the Table 1.

Table 1. Summary of studies on DL for IoT security

Attacks	Layers	Methods Implemented	Performance	Reference Papers
False Data	Perception Layer	Conditional Deep belief network	Temporal attack patterns	[28]
Spoofing	Perception layer	Virtual Channel space and Machine learning	Inspecting Valid device’s virtual channel characteristics.	[29]
Physical attacks	Perception Layer Application Layer	CNN based Power disaggregation and Prediction	Energy Anomaly	[33]
Intrusion detection	Perception Layer	DL based authentication(DNN,CNN,CPNN)	Spatial Diversity	[27]
Malware attacks	Network	Auto Encoders	Normal and	[31]

ISSN: 2233-7857 IJFGCN

	Layer		anomalous traffic features extraction	
Botnet	Network Layer	LSTM-RNN	Malicious behavior of nodes	[32]
Impersonation	Network Layer	Stacked Auto Encoder	Profiling deviation of normal and abnormal behavior	[35]
Routing attack	Network Layer	Deep Learning based attack detection	Increase in number of Packets received	[38]
Intrusion Detection	Transport Layer	Stacked auto encoder- ANN	Un-authorized Traffic	[37]
Distributed Denial of services	Transport Layer	ANN	Protocol Headers to learn the attacks.	[30]
Side channel attacks	Application Layer	CNN	Classification accuracy	[39]
Cyber Attacks	Application Layer	Stacked Auto encoder	False Positive,accuracy, Scalability	[36]

4. Deep Learning Methods:

4.1. Recurrent neural networks

RNN are essentially being deployed for predicting sequential data like in text prediction or speech recognition [16]. RNN encompasses a temporal layer which will take not just the current input but also the inferred foregoing input to apprehend sequential information and then assimilate all the past inputs with the current input in the hidden layers. Long Short Term Memory (LSTM), a variation of RNN consists of a cell that can store the previous information [32]. This feature of RNN can be implemented to detect the time series attacks in IoT devices as they generate sequential data [3].

4.2. Deep Autoencoders

These are the unsupervised neural network which converts the input into some form of code and then reconstructs it by learning meaningful features from the coded input. In [17] AEs are trained on benign datasets so whenever a malicious data is found in network AEs won't be able to reconstruct it. The model is successful in minimising the false prediction. AEs have paramount capability to extract the features for representation learning[17].By implementing multiple Deep autoencoders to form one model has been proposed to detect malicious javascript[14].

4.3. Restricted Boltzmann machine

RBM layers can be classified into two types i.e. hidden and visible layers and there is no connection between same layers. Contrastive divergence learning is used to train the RBM networks

[RBM]. The said property of RBM can be used to detect the anomaly in the dynamic and unlabelled data [18]. Though single RBM is not of very much use but they can be stacked together to form DBN.

4.4. Deep belief networks

DBN are made up of distinct layers of restricted Boltzmann machines stacked together and can be called as generative models [19]. These models can be trained by using greedy algorithms which can be applied to one individual layer at a time. DBN can be used to detect the anomalous code from the raw data in a standalone environment and can also be integrated with auto encoders to form a detection model [20]. DBN is an unsupervised training model that can be trained on unlabelled data but they can't be implemented on devices with constrained resources.

4.5. Generative adversarial network

GAN consists of generative and discriminative models [3] which are trained concomitantly using adversarial process. Generator network generates the data and the discriminator will predict whether it is a generated data or is from a real sample.GAN can be implemented to discriminate the anomalous behavior of the network from the normal one. A GAN framework to identify malicious network traffic is proposed in [21].

4.6. Convolutional Neural Network

CNN network contains alternate multiple convolutional and pooling layers for initial stage and then have fully connected layers.The network is characterized by sparse interaction and weight sharing because of the use of multiple kernels which are shared by all locales in the image[23].Multiple kernels having the same size are used to perform the convolution operation and the size of input is reduced in the pooling layer either by using max or average pooling. In max pooling the input is being divided into small non overlapping regions and a stride to find the maximum value from all the regions is done whereas in average pooling the average is taken for the values [22]. CNN can be used to detect the malwares in IoT devices as they can automatically comprehend features from the unprocessed data.CNN can be implemented to assimilate malware signatures from unprocessed data without requiring to hand code it. Disassembled code from an android app is treated as text for processing [15].

5. Conclusion

With the growth of the IoT industry the dependency on technology has begun to proliferate and the necessity to secure IoT devices has become the need of the hour.In addition to this a customized security for the devices has also become important owing to the heterogeneity of IoT ecosystem. A broad overview of various attacks on IoT devices with the ongoing research are discussed in this survey. Also, Deep Learning methods that can be used to develop robust analytical tools to enhance security are reviewed. Though many methodologies have been implemented, research attempts to secure the zero day attacks and a unified solution should be provided that can work irrespective of any platform for authorization, access control, and secrecy for clients and devices, clandestineness between devices and users.

References

[1] Xiao, L., Wan, X., Lu, X., Zhang, Y. Wu, D.: ‘IoT Security Techniques Based on Machine Learning’,2018, arXiv preprint arXiv:1801.06275.

[2] K. M. Sadique, R. Rahmani, P. Johannesson, "Towards Security on Internet of Things: Applications and Challenges in Technology", Procedia Computer Science, vol. 2018.

[3]M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, A survey of machine and deep learning methods for Internet of Things (IoT) security, 2018

[4]S. Babar, A. Stango, N. Prasad, J. Sen and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Chennai, 2011, pp. 1-5.

[5] Varadarajan, P., & Crosby, G. (2014, March). Implementing IPsec in wireless sensor networks. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on (pp. 1-5). IEEE.

[6] R. Roman, J. Zhou,J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[7] S. Chen, H. Xu, D. Liu, and B. Hu, "A vision of IoT: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349–359, Jul. 2014.

[8] M. Abomhara, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65-88, 2015.

[9] Bertino.E, Islam.N, "Botnets and internet of things security," Computer, vol. 50, no. 2, pp. 76-79, 2017.

[10] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep learning applications and challenges in big data analytics," Journal of Big Data, vol. 2, no. 1, p. 1, 2015.

[11] N. D. Lane et al., "Deepx: A software accelerator for low power deep learning inference on mobile devices," in Information Processing in Sensor Networks (IPSN), 2016 15th ACM/IEEE International Conference on, 2016, pp. 112: IEEE.

[12] H. Li, K. Ota, and M. Dong, "Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing," IEEE Network, vol. 32, no. 1, pp. 96-101, 2018.

[13]J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the edge: A scalable iot architecture based on transparent computing," IEEE Network, vol. 31, no. 5, pp. 96-105, 2017.

[14] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage Signaling Game-based Optimal Detection Strategies for Suppressing Malware Diffusion in Fog-Cloudbased IoT Networks," IEEE Internet of Things Journal, 2018.

[15] N. McLaughlin et al., "Deep android malware detection," in Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, 2017, pp. 301-308: ACM.

[16] A. Graves, A.-r. Mohamed, G. Hinton,"Speech recognition with deep recurrent neural networks," in Acoustics, speech and signal processing, IEEE international conference on, 2013, pp. 6645-6649: IEEE.

[17] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cybersecurity applications," in Neural Networks (IJCNN), 2017.

[18] U. Fiore, F. Palmieri, A. Castiglione, and A. De Santis, "Network anomaly detection with the restricted Boltzmann machine," Neurocomputing, vol. 122, pp. 13-23, 2013.

[19] H. F. Nweke, Y. W. Teh, M. A. Al-garadi, and U. R. Alo, "Deep Learning Algorithms for Human Activity Recognition using Mobile and Wearable Sensor Networks: State of the Art and Research Challenges," Expert Systems with Applications, 2018.

[20] Li, Yuancheng & Ma, Rong & Jiao, Runhai. "A Hybrid Malicious Code Detection Method based on Deep Learning". International Journal of Software Engineering and Its Applications. 9. 205-216, 2015.

[21] R. E. Hiromoto, M. Haney, and A. Vakanski, "A secure architecture for IoT with supply chain risk management," in Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 9th IEEE International Conference on, 2017, vol. 1, pp. 431- 435: IEEE

[22] D. Scherer, A. Müller, and S. Behnke, "Evaluation of pooling operations in convolutional architectures for object recognition," in International conference on artificial neural networks, 2010, pp. 92-101: Springer.

[23] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, Deep learning. MIT press Cambridge, 2016.

[24] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety,

security, and sustainability of mission-critical cyber–physical systems," Proceedings of the IEEE, vol. 100, no. 1, pp. 283-299, 2012.
[25]F. Y. Yavuz, "Deep learning in cyber security for internet of things," 2018. (Book)
[26]C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80-84, 2017.
[27] Liao, R.-F.; Wen, H.; Wu, J.; Pan, F.; Xu, A.; Jiang, Y.; Xie, F.; Cao, M. Deep-Learning-Based Physical Layer Authentication for Industrial Wireless Sensor Networks. Sensors 2019, 19, 2440.
[28] Y. He, G. J. Mendis and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2505-2516, Sept. 2017.
[29] N. Wang, L. Jiao, P. Wang, M. Dabaghchian and K. Zeng, "Efficient Identity Spoofing Attack Detection for IoT in mm-Wave and Massive MIMO 5G Communication," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6.
[30] Saied, Alan & Overill, Richard & Radzik, Tomasz. (2015). Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing. 172. 10.1016.
[31] M. Yousefi-Azar, V. Varadharajan, L. Hamey and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," 2017 International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, 2017, pp. 3854-3861.
[32] P. Torres, C. Catania, S. Garcia, and C. G. Garino, "An analysis of Recurrent Neural Networks for Botnet detection behavior," in Biennial Congress of Argentina (ARGENCON), 2016 IEEE, 2016, pp. 1-6: IEEE.
[33] F. Li, Y. Shi, A. Shinde, J. Ye and W. Song, "Enhanced Cyber-Physical Security in Internet of Things Through Energy Auditing," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5224-5231, June 2019.
[34] J. Granjal, E. Monteiro, and J. S. Silva, “Security for the internet of things: A survey of existing protocols and open research issues,” IEEE Communications Surveys Tutorials, vol. 17, pp. 1294–1312.
[35] L. Li, H. Xiaoguang, C. Ke and H. Ketai, "The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid," 2011 6th IEEE Conference on Industrial Electronics and Applications, Beijing, 2011, pp. 789-793.
[36] A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," in IEEE Communications Magazine, vol. 56, no. 2, pp. 169-175, Feb. 2018.
[37] Aminanto, Muhamad Erza and Kwangjo Kim. Deep Learning-based Feature Selection for Intrusion Detection System in Transport Layer 1, 2016.
[38] Yavuz, F. Y., nal, D., & Gl, E. (2018). Deep learning for detection of routing attacks in the internet of things. International Journal of Computational Intelligence Systems, 12(1), 39-58
[39] S.Picek, I. Samiotis, A. Heuser, J.Kim, S. Bhasin,Axel L.”On the Performance of Convolutional Neural Networks for Side-channel Analysis.”SPACE 2018 – Int. Conf. on Security, Privacy, and Applied Cryptography Engineering, Dec 2018, Kanpur, India. pp.157-176.