International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 06, June 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

A Survey on Intrusion Detection Techniques in IOT Networks.

Mrs. Nilofar S. Hunnargi[1] , Dr. Ajay D. Jadhav[2]

[1]*E&TC Engineering Department ATS's SBGI Miraj,India.*

[2]*Principal Dnyanshree Institute of Engineering & Technology [DIET], Satara, India.*

Abstract:

In the Internet of Things (IoT) systems number of user-specific things areconnected through the Internet. This focuses more attention on the security of these devices for authenticated access. Thesecurity of the system should provide better and more reliable services to authenticated users or application-oriented accesses. This paper presents a survey of various techniques for detection and prevention of attacks, effects of attacks on IOT devices, Wi-Fi networks, network traffic, etc. proposed by researchers. The survey elaborated on various performance evaluation strategies employed for different attack types with different performance metrics such asaccuracy, detectionrate, false alarm rate, etc. The performance metricslike accuracy is ranging up to 99.2. The survey emphasizes that most systems are vulnerable to Denial of Service (DoS) type of attacks and the deep learning-based strategic understanding techniques provide better solutions as well as the platform for further research in the same field.

Keywords:*DDOS Attack, Intrusion Detection Systems,IOT Networks,Machine Learning.*

I. Introduction

A network intrusion refers to any unauthorized activity on a digital network. Network intrusions often involve stealing valuable network resources and almost always jeopardize the security of networks and/or their data. An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

IoT network security is often the most essential need considering the huge rise in internet-connected devices day by day. The security algorithm development should essentially consider the attack types to define the attack prevention strategy. The main aspect of this survey is to study and analyze IoT security algorithms and performance metrics, proposed by various researchers.

II. Literature Survey

The literature survey is focused on various security algorithms,developed for making the system secure againstDistributed Denial of Service (DDoS) attacks.Most of the algorithms

are based on deep learning approaches.

In [1], the authors present a deep-learning-based classifier that learns hardware imperfections of low-power radios that are challenging to emulate, even for high-power adversaries. Authors build aLong Short-Term Memory (LSTM) framework, specifically sensitive to signal imperfections that persist over long durations. An experimental result from a test bed of 30 low-power nodes demonstrates high resilience to advanced software radio adversaries. Here classification accuracy is checked as Performance metricsand for 2 layer LSTM model, 99.58% accuracy is achieved. In [2], the authors present a wireless device identification platform to improve Internet of things (IoT) security using deep learning techniques. Deep learning is a promising method for obtaining the characteristics of the different RF devices through learning from their RF data. Specifically, three different deep learning models, namely Deep Neural Network (DNN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) are considered here to identify wireless devices and distinguish among wireless devices from the same manufacture. As a case study, large data sets of RF traces from six "identical" ZigBee devices are collected using a USRP-based test bed. The authors captured RF data across a wide range of Signal-to-Noise Ratio (SNR) levels to guarantee the resilience of the author's proposed models to a variety of wireless channel conditions in practical scenarios. RF fingerprinting to distinguish between legitimate devices and adversaries can be seen as an intrusion detection system (IDS) where impersonate attacks can be detected by the model. By detecting a malicious device that tried to masquerade itself as a legitimate one, here it declares an alarm for a security breach. It enhances the wireless network security and improves the overall service accessibility, authentication, and integrity. Experimental results demonstrate the high accuracy of deep learning methods for wireless device identification that potentially could enhance IoT security.

In [3], the authors have shown a method of a blockchain-enabled efficient data collection and secure sharing scheme combining Ethereumblockchain and deep reinforcement learning (DRL) to create a reliable and safe environment. In this scheme, DRL is used to achieve the maximum amount of collected data, and blockchain technology is used to ensure the security and reliability of data sharing. Extensive simulation results demonstrate that the proposed scheme can provide a higher security level and stronger resistance to attack than a traditional database-based data sharing scheme for different

levels/types of attacks.

In [4], the authors have given a distributed deep learning scheme of cyber-attack detection in fog-to-things computing. The new and emerging IoT applications require novel cyber security controls, models, and decisions distributed at the edge of the network. The author also has addressed the existing cryptographic solutions on the traditional Internet, factors such as system development flaws, increased attack surfaces, and hacking skills have proven the inevitability of detectionmechanisms. Authors have analyzed that the traditional approaches such as classical machine-learning-based attack detection mechanisms have been successful in the last decades, but it has already been proven that they have less accuracy and scalability for cyber-attack detection in distributed nodes such as IoT. Authors suggest that the proliferation of deep learning and hardware technology advancement could pave the way to detecting the current level of sophistication of cyber-attacks in edge networks. The application has already been successful in big data areas,deep networks can be applied successfully so fog-to-things computing can be the best-suited approach for attack detection because a massive amount of data produced by IoT devices enables deep models to learn better than shallow algorithms. The author's experimentation shows that deep models are superior to shallow models in detection accuracy, false alarm rate, and scalability.

In [5], the authors have presented the architecture of cloud-assisted IoT applications for smart cities, telemedicine, and intelligent transportation system. Authors have considered current security threat obstacles to the adoption of IoT technology in many areas. Authors investigate the security threats and attacks due to unauthorized access and misuse of information collected by IoT nodes and devices. Further, the authors describe the possible countermeasure to these security attacks.

In [6], the authors have given the method of Deep-Feature Extraction and Selection (D-FES), which combines stacked feature extraction and weighted feature selection. The stacked auto encoding is capable of providing representations that are more meaningful by reconstructing the relevant information from its raw inputs. Authors then combine this with modified weighted feature selection inspired by an existing shallow-structured machine learner. The authors finally demonstrate the ability of the condensed set of features to reduce the bias of a machine learner model as well as the computational complexity. The author's experimental results on a well-referenced Wi-Fi network benchmark dataset,

namely, the Aegean Wi-Fi Intrusion Dataset (AWID), prove the usefulness and the utility of the proposed D-FES by achieving a detection accuracy of 99.918% and a false alarm rate of 0.012%, which is the most accurate detection of impersonation attacks reported in the literature.

In [7], the authors have addressed the need for an automated testing framework to help security analysts to detect errors in learning-based IoT traffic detection systems. The authors have given the method of a testing framework for learning-based IoT traffic detection systems, TLTD. With genetic algorithms, TLTD can generate opposing samples for IoT traffic detection systems and may perform a black-box test on the systems.

In [8], the authors have given research work that aims to co-develop a consumer security index (CSI), with consumers and security experts, to help consumer decision-making and encourage greater security provision in the manufacture of IoT devices. In this paper, the authors focus on the methodology for the development of the index. Through a focus group with IoT security experts, the first part will identify security features that consumer IoT devices should provide. The second part will employ an online survey to identify consumer preferences concerning the disclosure of security and privacy features that devices provide, and focus groups will help to co-design the CSI by discussing the information value, appeal, and likely engagement of a security index label. The third part will develop a matrix of different classes of IoT devices manually coded according to the CSI for a sample of devices. The last and fourth parts will explore the use of natural language processing to extract data from device user manuals to identify what information is communicated about the security features and which crime prevention messaging is provided by manufacturers. Here CSI is co-designed with experts and consumers. The ultimate aims are to encourage the employment of the index to help inform consumer choice, and to lever market action so that IoT devices are shipped with in-built security measures.

In [9], the authors have provided a review of the main IoT security standards and guidelines that have been developed by formal standardization organizations and transnational industry associations and interest alliances to date. The review makes three main contributions to the study of current IoT standards-development processes. First, governments and regulatory agencies in the EU and the US are increasingly considering the promotion of baseline IoT security requirements, achieved through public procurement

obligations and cyber security certification schemes. Second, the analysis reveals that the IoT security standards landscape is dominated by de facto standards initiated by a diverse range of industry associations across the IoT ecosystem. Third, the paper identifies several key challenges for IoT security standardization, most notably: a) the difficulty of setting a baseline for IoT security across all IoT applications and domains; and b) the difficulty of monitoring the adoption, implementation, and effectiveness of IoT security standards and best practices. The paper consequently contributes to a better understanding of the evolution of IoT security standards and proposes a more coherent standards development and deployment approach

In [9], the authors have provided a review of the most IoT security standards and guidelines that are developed by formal standardization organizations and transnational industry associations and interest alliances to this point. The review makes three main contributions to the study of current IoT standards-development processes. First, governments and regulatory agencies within the EU and also the US are increasingly considering the promotion of baseline IoT security requirements, achieved through public procurement obligations and cyber security certification schemes. Second, the analysis reveals that the IoT security standards landscape is dominated by de facto standards initiated by a various range of industry associations across the IoT ecosystem. Third, the paper identifies a variety of key challenges for IoT security standardization, most notably: a) the issue of setting a baseline for IoT security across all IoT applications and domains; and b) the problem of monitoring the adoption, implementation, and effectiveness of IoT security standards and best practices. The paper consequently contributes deep insights into the evolution of IoT security standards and suggests a more coherent standards development and deployment technique.

In [10], the authors have presented the IoT enabled with a smart security system for the home. To provide security to the home this paper is helpful. When the intruders enter the house, an image of the intruder is captured by the system, even if the intruder escapes Police need to catch the intruder to recover the stolen things which need the picture of the intruder to the police. The system presented in the paper captures the picture of the intruder and sends it to the authorized mail through the internet over Simple Mail Transfer Protocol (SMTP). So security in the home is provided more effectively in the smart way of communicating things. Home appliances are smartly automated to reduce the human effort

for intelligent decisions with the help of the Internet Of Things (IoT). The product is designed to provide security and control home appliances in the house by the owner through IoT servers. The microcontroller used here is Raspberry Pi3 for all processing and controlling operations. Various sensors such as LM35 a temperature sensor, Light Dependent Resistor, PIR sensor with a magnetic door switch, and smoke sensor are interfaced to pi General Purpose Input Output port pins through Analog to Digital Converter module along with a camera and LAN connection is interfaced to the pi board.

In [11], the authors have presented a PUF-based authentication protocol that can enable easy and secure identification of devices in an IoT environment. When any narrowband Tx device modulates digital data, the resulting wave inherently contains device-specific unique analog/RF properties such as frequency offset and I-Q imbalance. These non-idealities are usually discarded or minimized at the receiver end as they are irrelevant in terms of the transmitted information. However, if those non-idealities are effectively harnessed using an in-situ machine learning framework at the Rx, the entropy information can be extracted for each of these transmitters, which leads to secure identification. Physical unclonable functions (PUF) in silicon exploit die-to-die manufacturing variations during fabrication for uniquely identifying each die. Since it is practically a hard problem to recreate exact silicon features across dies, a PUF-based authentication system is robust, secure, and cost-effective, as long as bias removal and error correction is taken into account. Authors have shown utilization of the effects of inherent process variation on analog and radio-frequency (RF) properties of multiple wireless transmitters in a sensor network, and detect the features at the receiver using a deep neural network-based framework. The proposed mechanism/framework, called RF-PUF, harnesses already- existing RF communication hardware and does not require any additional PUF-generation circuitry in the Transmitter for practical implementation. Simulation results indicate that the RF-PUF framework can distinguish up to 10000 transmitters (with standard foundry defined variations for a 65 nm process, leading to non-idealities such as LO offset and I-Q imbalance) under varying channel conditions, with a probability of false detection < 10-3.

In [12], the authors have given a methodology to leverage readable strings in binaries to calculate the similarities between different IoT firmware. Due to the extensive code reuse and the widespread use of third-party SDKs, homologous binaries are widely found in IoT firmware. Once a vulnerability is found in one firmware, other firmware

sharing a similar piece of code is at high risk. Thus, homologous binary search is of great significance to IoT firmware security analysis. However, there are still no scalable and efficient homologous binary search methods for IoT firmware. The time complexity of the state-of-the-art method is O(N), and it is not scalable for large-scale IoTfirmware. In this paper, the authors have given design, implement, and evaluate a scalable and efficient homologous binary search scheme (termed IHB) for IoT firmware with time complexity. Furthermore, the authors employ a string filter and the string-based MinHash to achieve both accuracy and efficiency. The authors test both author's scheme and the state-of-the-art methods on a real dataset containing 1024 binary files. The results show that the author's method is three orders of magnitude more efficient than the existing methods. Meanwhile, the author's method has a higher true positive rate (92.88%) and a lower false-positive rate (2.83%). In the interest of open science, authors also make author's tools and datasets publicly available to seed future improvements.

In [13], the authors found the functional requirements within the IoT information security sharing system to verify the functions to be performed between the individuals within the reference model of the IoT information security sharing system. IoT is being applied to varied industries, and market activation is fully swinging in the home- appliance, medical, and transportation fields closely associated with life. Authors have addressed current security vulnerabilities of assorted industries, reported in various fields, but only security requirements exist, but there's no technical countermeasure, and policy issues and security matters are discussed only within the field of standardization. Authors also deduce that to address the widespread infringement accidents, an information security sharing system within the IoT environment which will be applied directly within the field is required.

In [14], the authors present basic elements of IoT models and supply situation assessment for IoT applications. Authors have highlighted the protection enhancement measures for the IoT applications supported by the three domains (local, transfer, and data storage) of the IoT model. The author has addressed challenges in IoT systems in terms of the confidentiality, authenticity, and integrity of the info sensed, collected, and exchanged by the IoT objects. These challenges make IoT deployments extremely liable to differing kinds of security attacks, leading to insecure IoT environments.

In [15], the authors have given the on-demand security configuration technique that

can be configured for required security functions and reorganized them without recreating the device image. For a massive amount of devices in IoT, with the help of this approach, if there is a change in this security service, the author's technique can substitute the old modules for new ones without regenerating the device image.

In [16], the authors have introduced a multi-hop routing protocol that enables secured IoT devices' communication. The routing protocol enables the IoT devices to authenticatebefore forming a new network or joining an existing network. The authentication uses multi-layer parameters to enhance the security of the communication. The given routing protocol embeds the multi-layer parameters into the routing algorithm, thus combining the authentication and routing processes without incurring significant overheads. The multi-layer parameters include a unique User-Controllable Identification, users' pre-agreed application(s), and a list of permitted devices, thus saving resources by maintaining smaller routing information. Experimental and field tests were conducted with results showing that the author's secure multi-hop routing is suitable to be deployed for IoTcommunication. In [17], the author has explored the challenges in circuit designs of emerging memory devices for application in nonvolatile logic, security circuits, and CIM for deep neural networks (DNN). Emerging non-volatile memory (NVM) devices are not limited to building nonvolatile memory macros. They can also be used in developing nonvolatile logics (nvLogics) for nonvolatile processors, security circuits for the internet of things (IoT), and computing-in-memory (CIM) for artificial intelligence (AI) chips. Several silicon-verified examples of these circuits are reviewed in this paper. In [18], the author has addressed the deep learning approach for security systems. Several industries in many different domains are looking at deep learning as a way to take advantage of the insights in their data, to improve their competitiveness, open up novel business possibilities, or resolve problems thought to be impossible to tackle. The large scale of the systems where deep learning is applied and the need of preserving the privacy of the used data have imposed a shift from the traditional centralized deployment to a more collaborative one. Providing security can be costly in terms of higher energy consumption, calling for wise use of these protection means. The author's work exploits game theory to model interactions among collaborative deep learning nodes and to decide when using actions to support security Enhancements.

In [19], the authors try and bring order to the IoT security panorama by providing a

taxonomic analysis from the angle of the three main key layers of the IoT system model: Perception, Transportation, and Application levels. Social Internet of Things (SIoT) may be a new paradigm where IoT merges with Social Networks, allowing people and devices to interact, and facilitating information sharing. However, security and privacy issues are an exceptionalchallenge for IoT but they're also enabling factors to make a "trust ecosystem". Authors have shown that the intrinsic vulnerabilities of IoT devices, with limited resources and heterogeneous technologies, along with the shortage of specifically designed IoT standards, represent a fertile ground for the expansion of specific cyber threats. As a result of the analysis, the authors have highlighted the foremost critical issues to guide future research directions.

In [20], the authors have given a methodology that is intended to be used for the different experiments that are proposed in the scope of the ARMOUR project for assessing the fulfillment of several security aspects. The work presented provides a design of a certification methodology for IoT, paying attention to the test-based risk assessment phase to empower testers with the ability to assess security solutions for large-scale IoT deployments. The approach is an instantiation of the Risk-based Security Assessment presented by ETSI based on the ISO 31000, and it is built on top of different technologies and approaches for security testing and risk assessment adapted to the IoT landscape. The author has a direction to be used as a baseline to build a new security certification and labeling approach for IoT devices.

III. Conclusion

This paper provides a strategic understanding of security in IoT systems. The methods used for detection using deep learning show feature extraction strategies and updating the existing feature set for detecting further modified strategies of attacks. The paper may remain helpful for further research in the field of IoT security.

[1] R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. F. Moura, "A Deep Learning Approach to IoT Authentication," *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, 2018, pp. 1-6. DOI: 10.1109/ICC.2018.8422832

[2] H. Jafari, O. Omotere, D. Adesina, H. Wu and L. Qian, "IoT Devices Fingerprinting Using Deep Learning," *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, USA, 2018, pp. 1-9. DOI: 10.1109/MILCOM.2018.8599826

[3] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning," in *IEEE Transactions on Industrial Informatics*. DOI: 10.1109/TII.2018.2890203

[4] 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. DOI: 10.1109/MCOM.2018.1700332

[5] Alsaidi and F. Kausar, "Security Attacks and Countermeasures on Cloud Assisted IoT Applications," *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, 2018, pp. 213-217. DOI: 10.1109/SmartCloud.2018.00043

[6] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo and K. Kim, "Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621-636, March 2018.
DOI: 10.1109/TIFS.2017.2762828

[7] Xiaolei Liu, Xiaosong Zhang, NadraGuizani, Jiazhong Lu, Qingxin Zhu, Xiaojiang Du, "TLTD: A Testing Framework for Learning-Based IoT Traffic Detection Systems", Sensors 2018, 18, 2630; doi:10.3390/s18082630

[8] J. M. Blythe and S. D. Johnson, "The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-7. DOI: 10.1049/cp.2018.0004

[9] I. Brass, L. Tanczer, M. Carr, M. Elsden and J. Blackstock, "Standardising a moving target: The development and evolution of IoT security standards," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-9. DOI: 10.1049/cp.2018.0024

[10] M. L. R. Chandra, B. V. Kumar, and B. SureshBabu, "IoT enabled home with smart security," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 1193-1197. DOI: 10.1109/ICECDS.2017.8389630

[11] B. Chatterjee, D. Das and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning," 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, 2018, pp. 205-208. DOI: 10.1109/HST.2018.8383916

[12] Y. Chen, H. Li, W. Zhao, L. Zhang, Z. Liu, and Z. Shi, "IHB: A scalable and efficient scheme to identify homologous binaries in IoT firmware," 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, 2017, pp. 1-8. DOI: 10.1109/PCCC.2017.8280478

[13] J. Choi, Y. Shin, and S. Cho, "Study on information security sharing system among the industrial IoT service and product provider," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 551-555. DOI: 10.1109/ICOIN.2018.8343179

[14] P. K. Chouhan, S. McClean, and M. Shackleton, "Situation Assessment to Secure IoT Applications," 2018 Fifth International Conference on Internet of Things: Systems, Management, and Security, Valencia, 2018, pp. 70-77. DOI: 10.1109/IoTSMS.2018.8554802

[15] B. Chung, J. Kim and Y. Jeon, "On-demand security configuration for IoT devices," 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2016, pp. 1082-1084. DOI: 10.1109/ICTC.2016.7763373

[16] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 428-432. DOI: 10.1109/WF-IoT.2014.6803204

[17] C. Dou et al., "Challenges of emerging memory and memristor-based circuits: Nonvolatile logics, IoT security, deep learning, and neuromorphic computing," 2017 IEEE 12th International Conference on ASIC (ASICON), Guiyang, 2017, pp. 140-143. DOI: 10.1109/ASICON.2017.8252431

[18] C. Esposito, X. Su, S. A. Aljawarneh and C. Choi, "Securing Collaborative Deep Learning in Industrial Applications Within Adversarial Scenarios," in IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4972-4981, Nov. 2018. DOI: 10.1109/TII.2018.2853676

[19] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug. 2018. DOI: 10.1109/JIOT.2017.2767291

[20] S. N. M. García, J. L. Hernández-Ramos and A. F. Skarmeta, "Test-based risk assessment and security certification proposal for the Internet of Things," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 641-646. DOI: 10.1109/WF-IoT.2018.8355193