Review on Trust Building Algorithms in IoT Security

Haoxiang Wang

Director and Lead Executive Faculty Member, GoPerception Laboratory, Cornell University, Ithaca, USA

E-mail: wanghaoxiang1102@hotmail.com

Abstract

IoT security is a combination of physical device security and network security. The objective of the IoT security module is to hide the network from communication vulnerabilities between the transmitter module and the server. Also, the security algorithms are designed to protect the systems from software attacks and physical hardware attacks. The paper explores the ongoing advancements and research in the field of IoT security by analyzing the research limitations and issues of the existing models. The research gaps identified from the literature analysis explores the way where the research on IoT security must be narrowed. Moreover, this paper projects the evolution of security threats in the IoT network, along with the analysis of deep learning models in estimating such threats.

Keywords: IoT security, data normalization, network attacks, intrusion detection, IoT datasets

1. Introduction

IoT (Internet of Things) is a system that gives internet connectivity to mechanical or electrical modules for automation or monitoring purposes. Therefore, the information and status of the connected devices are forwarded continuously to the network layer. The connected devices are open to attacks, if they are not protected with a proper security algorithm. The term "IoT security" refers to the combined protection of the hardware and software modules incorporated with network connectivity. In recent days, all electronic gadgets starting from wrist watches to mobile phones are connected with internet and that makes the devices open to vulnerabilities and malwares. Public Key Infrastructure (PKI) and

DOI: https://doi.org/10.36548/jismac.2021.4.004
Received: 01.02.2022, received in revised form: 25.03.2022, accepted: 08.04.2022, published: 19.04.2022

Application Program Interface (API) are the most popular security systems enabled for IoT security application. However, the systems that are connected with Bluetooth and infrared communication, are also considered as IoT devices and that gives challenges while designing an IoT security tool. Some of the common causes for IoT security challenges are discussed below [1, 2].

1.1 Remote access

Most of the IoT devices are designed to access from remote places. The amount of security problem gets increased with respect to the amount of entry points permitted in an IoT device. Hence the phishing model attacks are very effective in IoT devices. Therefore, in some cases the time permitted for internet connectivity is limited for IoT devices [3].

1.2 Absence of industrial precautions

Machines and control units available in the industrial environment are connected with internet access via Wi-Fi to minimize the wiring and hardware connections. It is managed by limiting the network connection inside the factory or industry. This improves the efficiency of the production line and minimizes the installation cost. However, the connected devices are mostly placed without any security frameworks, and the absence of security feature may increase the chances of data breach and device hacking at any time [4].

1.3 Resource limitation

Generally, the IoT devices are not equipped with any peripheral unit for running the security algorithm. So it needs to give up its performance while implementing it with a security protocol. The devices that are implemented for data computation application may have some free space in their module for running the security algorithm [5].

2. Related Work

2.1 Types of IoT attacks

The IoT devices are open to the attacks mentioned in Figure 1, where the communication attack is the most common attack that breaches the data transmitted from device to device on wireless medium. This is enabled by hacking the authorization of the IoT device. Communication attacks can be tackled by giving different authorization protocol for all the connected devices, but practically the systems that are connected with large quantity of devices are operated with same authorization methods and passwords which increases the chances of communication attacks. The security attacks are also insisted in IoT devices by detecting the weak points of the network. If a device among the system that is connected with more devices has some technical flaws inside, that allows the security threat to all the connected devices [6, 7]. Similarly, the abnormal computational load in such heavily connected system may also make the devices to identify the involved threats.

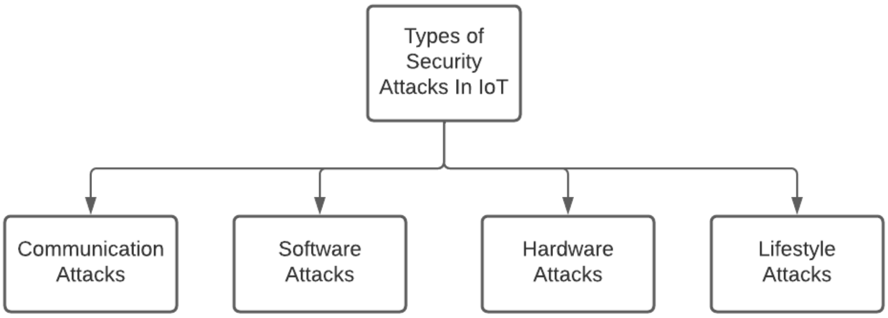

Figure 1. Common types of IoT attacks

The threat detection software which is placed without regular update may also lead the system to be open for security attacks. The latest types of attacks and vulnerabilities may not be even visible in such cases after long time. It also allows the hacker to manipulate the decision taken by the operating software inside the system. The IoT devices are also heavily open to human error during operation. In some cases, the system connected to open or unsafe network also welcomes the hackers to reach their destiny. The attackers may reach to the algorithms stored in the hardware when the threat is not identified at the right time. This may lead to serious issues like hardware hacking or system operational blocking. In most of the industrial application, the IoT devices are operated by a single-handed user [8, 9]. The interchangeability of operation may also increase the human error during the maintenance procedure. The hacking procedure implemented due to human error is also called as lifestyle attack.

2.2 Methodologies behind software protection

The software included in the IoT devices make a connecting platform between the hardware and the networking medium. A failure in software protection may result in the connected system being open for data loss [10]. The most common procedures followed for the IoT device software protection is listed below.

- Password Protection: A confidential password is required for accessing the software modules.
- Software Restrictions: The main and important features available in the software devices need to be disconnected from the internet connection.
- Firewall Block: Firewall block is required for sensitive algorithms running behind the software.
- Updates: Automate the software update process or the user must verify it regularly.
- Inspection: Periodic inspection is required for the system although there is no serious issue detected.

2.3 Methodologies behind network protection

The network is the primary way for the hackers to reach the IoT system. Therefore the following protection techniques are implemented in the IoT models.

- Port Security: The network ports are expected to be blocked when not used. Regular verification is required for ensuring the port security.
- Firewalls: Updated firewall and anti-malware system need to be incorporated in the IoT devices.
- Block: A restriction algorithm regulates the accessibility of the system from unknown or untrusted IP addresses.
- Segmentation: Network segmentation is a method that restricts the access of certain hardware or devices connected in the same system.

3. Literature Review

Table 1 explores the attainments of the previous techniques on IoT security applications. The IoT intrusions are mostly identified with machine learning or deep learning models and its effectiveness are very high over the traditional methods. However, the deep learning and machine learning models require a huge data for training and validation process. Few list of datasets that are available for neural network training models are shown in table 2. In some cases, the cryptographic based techniques are implemented for storing the data in a secured manner. Very few algorithms are found with light weighted classifiers, that are not very efficient to other regular models.

Table 1. Literature review on the present trust building algorithms of IoT

First author name and citations	Methodology followed	Attainments
Sudhakaran [11]	Efficient Distributed Lightweight Authentication and Encryption	7% improvement over the previous Secure Authentication and Access Mechanism
Shafiq [12]	Correlation based feature selection approach	More than 96% accuracy attained on BoT-IoT dataset
Makkar [13]	Generalized Linear Model with Stepwise Feature Selection	91.8% accuracy on REFIT Smart Home dataset
Dinakarrao [14]	Lightweight rule-based JRip model	91.08% accuracy
Roy [15]	2-D Von-Neumann Cellular Automata based encryption model	Better energy consumption and 93.37 MSE achieved
Mohanty [16]	Efficient Lightweight integrated Blockchain method	Reduced 50% of the processing time
Dash [17]	Adaptive boosting ensemble learning-based approach	Claimed 100% accuracy on DS2OS dataset
Rahman [18]	Key scheduling technique using a 3-dimensional substitutional box	Achieved a better computational time of 911ms over the previous 3-dimensional key generation matrix
Pokhrel [19]	Gaussian Naïve Bayes	99.4% accuracy on real-time BoT-IoT dataset

Meshram [20]	A lightweight provably secure short digital signature technique	Ensured safe communication between the devices and achieved 7.29ms time for signing in and verification
Roy [21]	Programmable cellular automata based block cipher	Achieved a better runtime on image encryption technique
Shafiq [22]	Naive Bayes with 44 features on BoT IoT dataset	99.99% accuracy
Rathee [23]	Routed and handoff mechanism	Showed an improvement of 85% over the previous techniques
Fatani [24]	Alternative feature selection design	Attained maximum accuracy on particle swarm optimization model
Al [25]	Software defined networking controller with HTTP and OpenFlow protocol	Effective in addressing MITM attack

Table 2. Major Datasets available for neural network training and validations

Dataset	**Location**	**Features Counts**	**Sample data count**	**Description**
N-BAIoT	[26]	115	8,49,234	Dataset requires balancing process as the benign count is very less
IoT23	[27]	23	32,53,07,990	HTTP protocol details are not available in the dataset. Created with real time IoT applications
Bot-IoT	[28]	45	7,33,70,443	Dataset contains 6 recent most malicious data
CICIDS2017	[29]	80	28,30,743	Recent kind of attacks are available in the dataset but the information is not directly related to IoT alone

ISCX2012	[30]	8	24,50,324	Simulated data and does not contain recent malicious data
UNSW-NB15	[31]	49	25,40,044	Dataset contains DDoS attack data from network traffic
NSLKDD	[32]	43	1,48,517	Most utilized dataset having balanced sample
KDDCUP99	[33]	41	52,09,458	Oldest dataset and not made with IoT networks

4. Discussion

The datasets that are available for deep learning-based analysis does not have even amount of data on all classes. Therefore, the dataset requires a balancing or normalization step before going into the preprocessing algorithm. Basically the normalization algorithms are categorized as oversampling and undersampling algorithms. SMOTE and random oversampling are the most popular oversampling methods that improve the count of minor sample classes available in the dataset. The undersampling algorithms are utilized to delete the samples that belong to major class samples. Random undersampling, near miss undersampling and condensed nearest neighbor sampling are the methods widely used for the undersampling applications.

Preprocessing is a step that comes next to the normalization process for making corrections over the available sample on missing data and corrupted data. The missing data samples are generally dropped from the list and are manipulated in rare cases. Regression, clustering and binning methods are widely employed for attending the corrupted samples. The regression method may have a function to smooth the samples with one or more variables and the clustering method groups the data that belong to the same group and eliminates the same when it comes under any group. The binning method is one of the complicated methods that segments the information that lies inside the sample into separate part and regulates the segmented values individually.

Selecting the optimum features from the dataset improves the prediction accuracy of the classifiers. The supervised feature selection model is categorized as filter method, wrapper method and intrinsic method. The filter method extracts the useful features by correlating the information with the labels specified over the given data samples. The wrapper method works by making various combinations of features in the training process and provides the best combination as output for improving the accuracy of the classifiers. The intrinsic method combines both filter and wrapper method to provide a best outcome. The normalization, preprocessing and feature selection method which are made for a specific dataset may not be suitable for another dataset. Hence it is always a difficult task for creating a classifier or prediction model that suits for all the recent intrusions.

5. Conclusion

IoT systems are growing day by day and its requirements are not limited to any application. The IoT models are implemented in agriculture, medical and various data sharing fields due to its architectural simplicity and minimal cost. However, the architectural simplicity makes the IoT devices a questionable one in terms of security. Various types of intrusion detection methods are developed by the researchers and developers for IoT systems, however there is a research gap found in terms of achieving better accuracy rate and computational time. This paper identifies that the network and communication attacks are very common in IoT systems rather than the hardware and software attacks. The review work also indicates that the dataset availability in the present situation is not adequate for making an efficient deep learning-based prediction algorithm. Therefore, the need for a best-balanced dataset on each class is still an open requirement.

References

[1] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." *Computer networks* 148 (2019): 283-294.

[2] Minoli, Daniel, and Benedict Occhiogrosso. "Blockchain mechanisms for IoT security." *Internet of Things* 1 (2018): 1-13.

[3] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future generation computer systems* 82 (2018): 395-411.

[4] Román-Castro, Rodrigo, Javier López, and Stefanos Gritzalis. "Evolution and trends in IoT security." *Computer* 51, no. 7 (2018): 16-25.

[5] Assiri, Abeer, and Haya Almagwashi. "IoT security and privacy issues." In *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-5. IEEE, 2018.

[6] Shen, Yun, and Pierre-Antoine Vervier. "Iot security and privacy labels." In *Annual Privacy Forum*, pp. 136-147. Springer, Cham, 2019.

[7] Li, Xiang, Qixu Wang, Xiao Lan, Xingshu Chen, Ning Zhang, and Dajiang Chen. "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach." *IEEE Access* 7 (2019): 9368-9383.

[8] Zhang, Jiliang, and Gang Qu. "Physical unclonable function-based key sharing via machine learning for IoT security." *IEEE Transactions on Industrial Electronics* 67, no. 8 (2019): 7025-7033.

[9] Zhou, Wei, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved." IEEE Internet of things Journal 6, no. 2 (2018): 1606-1616.

[10] Li, Fangyu, Rui Xie, Zengyan Wang, Lulu Guo, Jin Ye, Ping Ma, and WenZhan Song. "Online distributed IoT security monitoring with multidimensional streaming big data." *IEEE Internet of Things Journal* 7, no. 5 (2019): 4387-4394.

[11] Sudhakaran, Pradeep. "Energy efficient distributed lightweight authentication and encryption technique for IoT security." *International Journal of Communication Systems* 35, no. 2 (2022): e4198.

[12] Shafiq, Muhammad, Zhihong Tian, Ali Kashif Bashir, Xiaojiang Du, and Mohsen Guizani. "CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques." *IEEE Internet of Things Journal* 8, no. 5 (2020): 3242-3254.

[13] Makkar, Aaisha, Sahil Garg, Neeraj Kumar, M. Shamim Hossain, Ahmed Ghoneim, and Mubarak Alrashoud. "An efficient spam detection technique for IoT devices using machine learning." *IEEE Transactions on Industrial Informatics* 17, no. 2 (2020): 903-912.

[14] Dinakarrao, Sai Manoj Pudukotai, Xiaojie Guo, Hossein Sayadi, Cameron Nowzari, Avesta Sasan, Setareh Rafatirad, Liang Zhao, and Houman Homayoun. "Cognitive and scalable technique for securing iot networks against malware epidemics." *IEEE Access* 8 (2020): 138508-138528.

[15] Roy, Satyabrata, Manu Shrivastava, Chirag Vinodkumar Pandey, Sanjeet Kumar Nayak, and Umashankar Rawat. "IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata." *Multimedia Tools and Applications* 80, no. 21 (2021): 31529-31567.

[16] Mohanty, Sachi Nandan, K. C. Ramya, S. Sheeba Rani, Deepak Gupta, K. Shankar, S. K. Lakshmanaprabu, and Ashish Khanna. "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy." *Future Generation Computer Systems* 102 (2020): 1027-1037.

[17] Dash, P.B., Nayak, J., Naik, B., Oram, E. and Islam, S.H., 2020. Model based IoT security framework using multiclass adaptive boosting with SMOTE. *Security and Privacy*, *3*(5), p.e112.

[18] Rahman, Ziaur, Xun Yi, Mustain Billah, Mousumi Sumi, and Adnan Anwar. "Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home." *Electronics* 11, no. 7 (2022): 1083.

[19] Pokhrel, Satish, Robert Abbas, and Bhulok Aryal. "IoT Security: Botnet detection in IoT using Machine learning." *arXiv preprint arXiv:2104.02231* (2021).

[20] Meshram, Chandrashekhar, Mohammad S. Obaidat, Jitendra V. Tembhurne, Shailendra W. Shende, Kailash W. Kalare, and Sarita Gajbhiye Meshram. "A lightweight provably secure digital short-signature technique using extended chaotic maps for human-centered IoT systems." IEEE Systems Journal 15, no. 4 (2020): 5507-5515.

[21] Roy, Satyabrata, Umashankar Rawat, Harsh Ajay Sareen, and Sanjeet Kumar Nayak. "IECA: an efficient IoT friendly image encryption technique using programmable cellular automata." *Journal of Ambient Intelligence and Humanized Computing* 11, no. 11 (2020): 5083-5102.

[22] Shafiq, Muhammad, Zhihong Tian, Yanbin Sun, Xiaojiang Du, and Mohsen Guizani. "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city." *Future Generation Computer Systems* 107 (2020): 433-442.

[23] Rathee, Geetanjali, Rajinder Sandhu, Hemraj Saini, M. Sivaram, and Vigneswaran Dhasarathan. "A trust computed framework for IoT devices and fog computing environment." *Wireless Networks* 26, no. 4 (2020): 2339-2351.

[24] Fatani, Abdulaziz, Abdelghani Dahou, Mohammed AA Al-Qaness, Songfeng Lu, and Mohamed Abd Elaziz. "Advanced feature extraction and selection approach using deep

learning and Aquila Optimizer for IoT intrusion detection system." *Sensors* 22, no. 1 (2021): 140.

[25] Al Hayajneh, Abdullah, Md Zakirul Alam Bhuiyan, and Ian McAndrew. "Improving internet of things (IoT) security with software-defined networking (SDN)." *Computers* 9, no. 1 (2020): 8.

[26] Meidan, Yair, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. "N-baiot—network-based detection of iot botnet attacks using deep autoencoders." *IEEE Pervasive Computing* 17, no. 3 (2018): 12-22.

[27] Stoian, Nicolas-Alin. "Machine Learning for anomaly detection in IoT networks: Malware analysis on the IoT-23 data set." Bachelor's thesis, University of Twente, 2020.

[28] Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset." *Future Generation Computer Systems* 100 (2019): 779-796.

[29] Panigrahi, Ranjit, and Samarjeet Borah. "A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems." *International Journal of Engineering & Technology* 7, no. 3.24 (2018): 479-482.

[30] Soheily-Khah, Saeid, Pierre-François Marteau, and Nicolas Béchet. "Intrusion detection in network systems through hybrid supervised and unsupervised machine learning process: A case study on the iscx dataset." In *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, pp. 219-226. IEEE, 2018.

[31] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." In *2015 military communications and information systems conference (MilCIS)*, pp. 1-6. IEEE, 2015.

[32] Revathi, S., and A. Malathi. "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection." *International Journal of Engineering Research & Technology (IJERT)* 2, no. 12 (2013): 1848-1853.

[33] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In *2009 IEEE symposium on computational intelligence for security and defense applications*, pp. 1-6. Ieee, 2009.

Author's biography

Haoxiang Wang is currently a director and lead executive faculty member of GoPerception Laboratory, Ithaca, USA. His research interest includes multimedia information processing, pattern recognition, machine learning, remote sensing image processing, and data-driven business intelligence. He has co-authored over 60 journal and conference papers in these fields on journals such as Springer MTAP, Cluster Computing, SIVP; IEEE TII, Communications Magazine; Elsevier Computers & Electrical Engineering, Computers, Environment and Urban Systems, Optik, Sustainable Computing: Informatics and Systems, Journal of Computational Science, Pattern Recognition Letters, Information Sciences, Computers in Industry, Future Generation Computer Systems; Taylor & Francis International Journal of Computers and Applications and conference such as IEEE SMC, ICPR, ICTAI, ICICI, CCIS, and ICACI.