IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

A Critical Review on Learning Behavior for Protection of User's Privacy using IOT

Shrikanta Kolay[1] and Dr. Tryambak Hiwarkar[2]
Research Scholar, Department of Computer Science& Engineering[1]
Professor, Department of Computer Science& Engineering[2]
Sardar Patel University, Balaghat, MP, India

Abstract: *Changes and improvements to human existence have been made possible by recent advancements in communication and information technology, notably the internet of things (IoT). The IoT system is vulnerable to cyber-physical security and privacy assaults such denial of service, spoofing, phishing, obfuscations, and jamming because of the widespread availability and rising demand for smart devices. Cyber dangers to IoT systems, such as eavesdropping, attacks, and more. The new threats to cyber-physical security cannot be effectively avoided or mitigated using the same old methods. Keeping IoT systems safe calls on security measures that are not only effective, but also flexible and up-to-date. Among the various approaches to cyber-physical system security, machine learning (ML) is widely regarded as the most cutting-edge and promising since it has spawned several new lines of inquiry into the problem (CPS). This literature study provides an overview of the structure of Internet of Things (IoT) systems, explores the many attacks that may be launched against them, and discusses the current thinking on how to best use machine learning to ensure the security and safety of IoT infrastructure. It also covers the probable future research obstacles that may arise while implementing security measures in IoT systems.*

Keywords: IoT System, Security Threats

I. INTRODUCTION

We have witnessed companies go from producing individual items to constructing the network of products known as the Internet of Things (IoT), and finally developing an intelligent network of products delivering a variety of beneficial online services . That every three minutes, two new devices are added to the Internet. A rise in overall network traffic is a direct consequence of the proliferation of connected devices and the Internet of Things. There are problems that have evolved as a result of this connectedness, such as protecting the privacy of users' data and authenticating their devices. One billion Yahoo accounts were hacked into in 2013 alone. There were attacks on 145 million eBay users in 2014. In 2017, personal information for 143 million of Equifax's customers was compromised continuing a disturbing pattern of more sophisticated hacks. As revealed in 2017, a toy sector worth $5 billion had 800,000 customer accounts hijacked. Over two million voice recordings were included, some of which were later taken for ransom. Recent history is littered with examples of cybersecurity catastrophes, such as widespread data leaks, vulnerabilities in billions of microchips, and the locking down of whole computer networks until ransom is paid. The number of security and privacy issues plaguing IoT devices grows by the day. As a result, security and privacy in complex and resource-constrained IoT contexts present significant issues that must be adequately addressed.The assaults against the IoT are becoming more complex with time, heightening the difficulty of maintaining its security.

Milosevic et al. [5] noted that high-powered machines, including desktops, may be able to identify malware with their access to advanced tools. But Internet of Things gadgets only have so much power.

Additionally, standard cybersecurity systems and software are insufficient for detecting modest attack variants or zero-day assaults as both need to be updated often. In addition, the vendor does not provide updates in real-time, which leaves the network open to attack. As well as enhancing the effectiveness of cybersecurity systems machine learning

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

(ML) algorithms may be used to enhance Internet of Things (IoT) infrastructure such as smart sensors and IoT gateways.

The research contributions of this survey are as follows:

We address IoT device attack surfaces, vulnerabilities, and security concerns, including network, physical service, cloud service, application interfaces, and web service.

- Comprehensive discussion and comparison of previous surveys, including a statistical summary of newly published publications on IoT security ML approaches.
- Incorporating current polls on financial damages from IoT security breaches and the potential growth of IoT devices.
- ML-based IoT security research issues and directions.

II. AN OVERVIEW OF IOT SYSTEM

The Internet of Things (IoT) is a cyber-physical system comprising sensors, GPS, near-field communication sensors, RFID, and emergency alarms and detectors. Real-time IoT devices gather, classify, communicate, interpret, and respond to their surroundings. These gadgets retain data on light intensity, sound, electrical use, temperature, chemical reactions, biological changes, etc. The IoT framework connects a heterogeneous cyber-physical system via machine-to-machine, man-to-man, and machine-to-machine interactions. The IoT system uses sensor networks, ubiquitous computing, internet protocols, communication technologies, and apps to make common objects smart. Physical devices and communication networks supply smart services and applications under the IoT concept. IoT systems have three layers: application, network, and presentation or physical . Figure 1 depicts IoT architecture and analysis. Figure 1's three-layer IoT architecture summarises the system's fundamental concept:

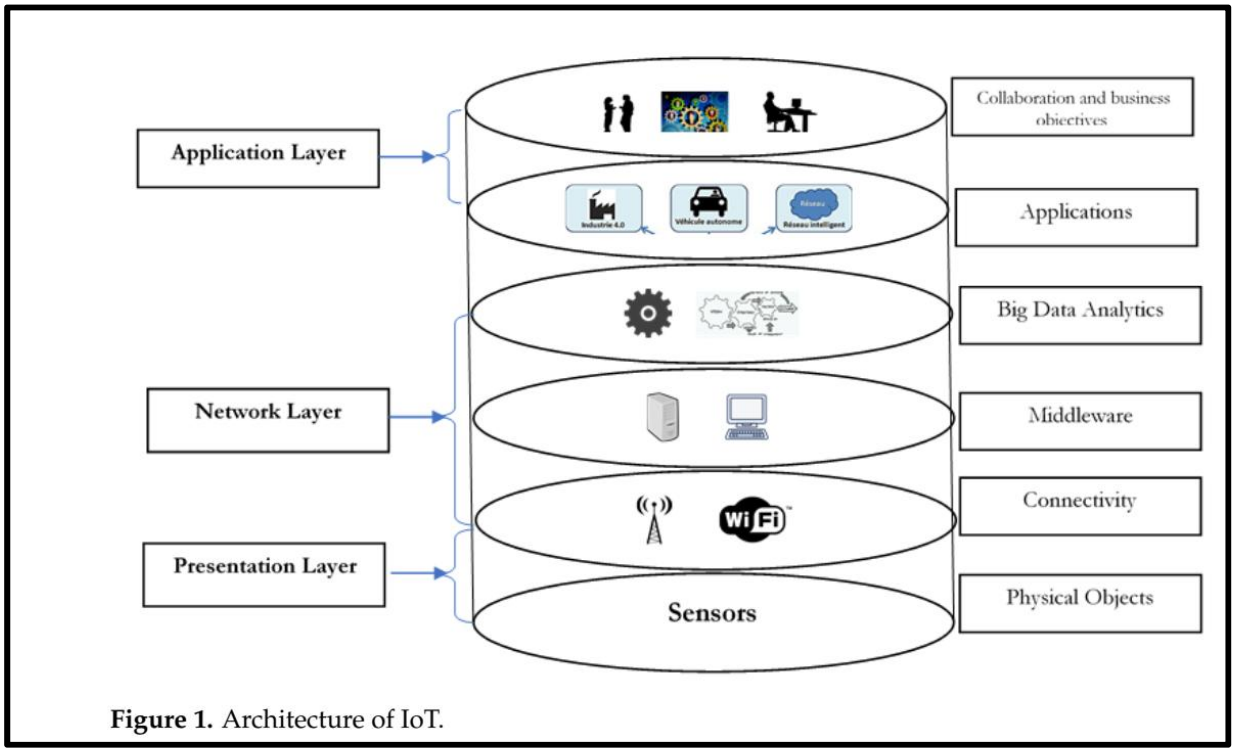

Figure 1. Architecture of IoT.

III. IoT SECURITY RISKS

Internet-connected devices link to their environment. The gadgets operate online in an undesirable manner. Thus, intruders and attackers can use susceptible IoT devices to eavesdrop and steal sensor credentials. Passive and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

aggressive dangers exist. Eavesdropping, a passive threat, uses system data without affecting system resources. An attacker/hacker attempts to change data and manipulate hardware. Sybil, DoS/DDoS, Trojans, spoofing, phishing, and smashing are active threats. Figure 2 shows security threats that might affect authorization, authentication, confidentiality, availability, integrity, and non-repudiation.

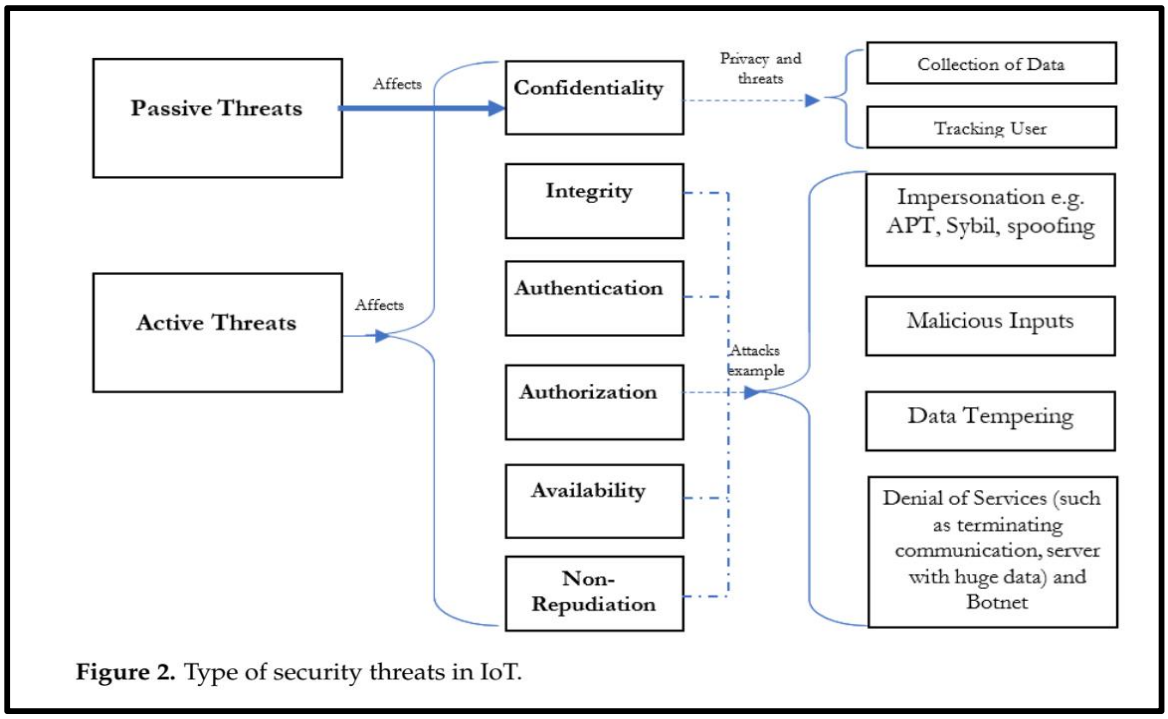

Figure 2. Type of security threats in IoT.

3.1. IoT Attack

This section discusses attack surfaces and dangers. Figure 3 illustrates IoT attack surfaces: network service, physical device, online and application services, and cloud service.

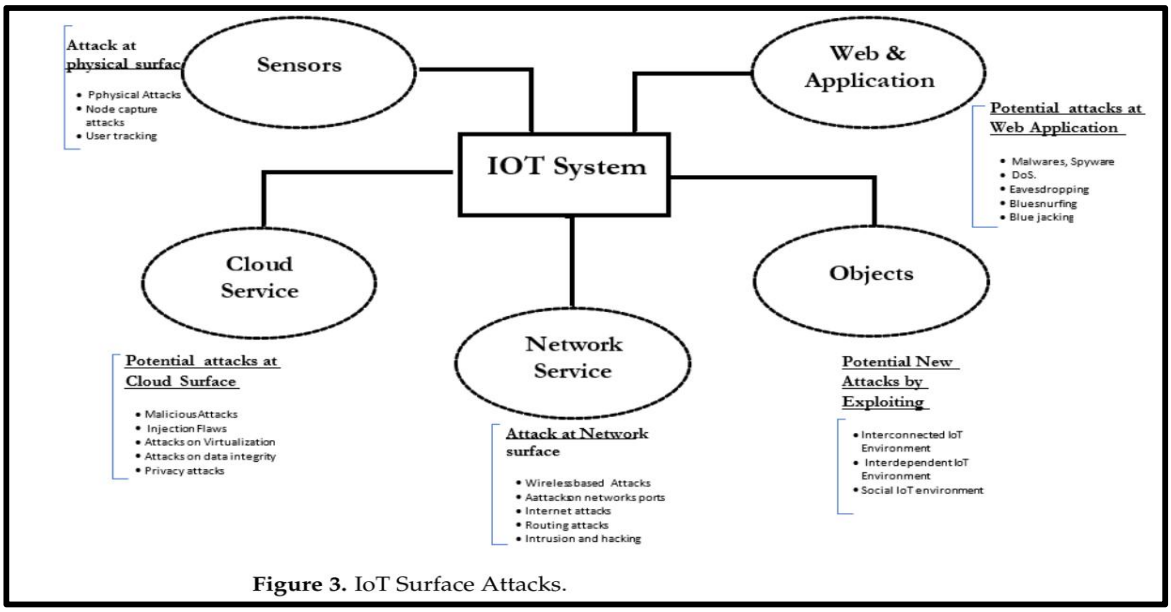

Figure 3. IoT Surface Attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

3.2 Security Threats

This section discusses attack surfaces and dangers. Figure 3 illustrates IoT attack surfaces: network service, physical device, online and application services, and cloud service. Two-person chat. Data leaks can compromise confidentiality, integrity, or availability. Privacy threats affect confidentiality. Threat. Security concerns influence data integrity and network availability. Figure 4 shows several IoT security and privacy issues.

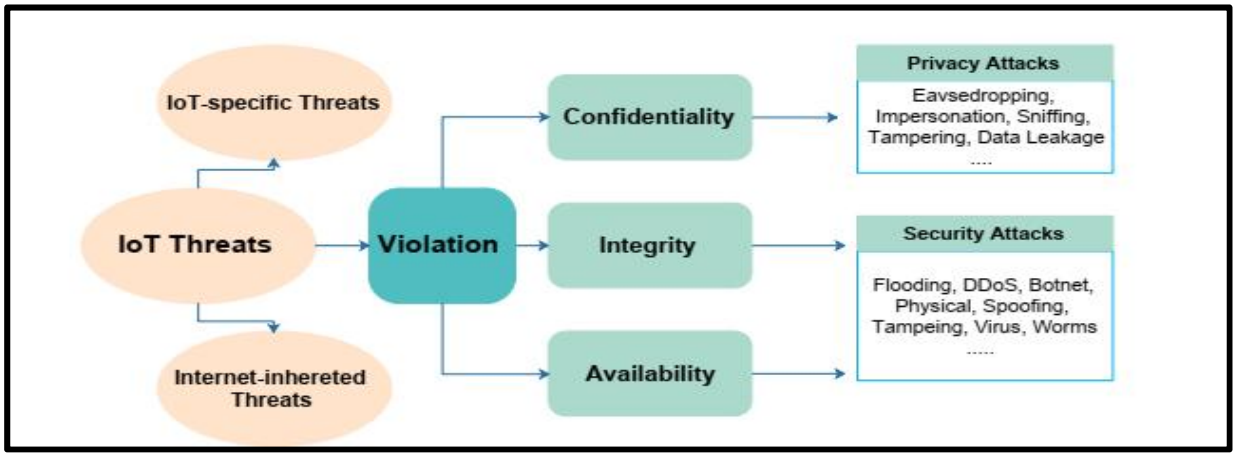

Figure 4: Types of IoT threats

3.3 Privacy Threats

Privacy attacks, such as sniffing, de-anonymization, and inference attacks, can pose a risk to IoT users and their data. The impact is on data privacy either when the data is at rest or in transit. Several types of intrusions into private space are discussed below.

MiTM: Privacy attacks, such as sniffing, de-anonymization, and inference attacks, can pose a risk to IoT users and their data. The impact is on data privacy either when the data is at rest or in transit. Several types of intrusions into private space are discussed below.

3.4 Data Privacy

Data privacy threats, like man-in-the-middle assaults, may be broken down into active and passive varieties (PDPA). Data leakage, data manipulation, identity theft, and re-identification [8] are all connected to data privacy. Attacks based on de-anonymization, location detection, and data aggregation comprise the backbone of re-identification methods, which are also known as inference attacks [8]. The primary objective of these assaults is to compromise several systems in order to divulge the identity of the targeted. The information may be used to create a false identity by some attackers [136]. Data tampering and other forms of data alteration fall under the category of ADPA, whereas re-identification and data leakage are examples of PDPA.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

Threat	Impact	Attack	Type	Layer of Impact	Solution
Security	Availability	DoS	Flooding	Physical, MAC	Multiple
			DDoS	Physical, MAC	Multiple
			Botnet	Physical, MAC	Multiple
		Physical	Damage	Physical	Physical Security
			Environmental	Physical	Shielding
			Power Loss	Physical	uninterrupted power
			Hardware Failure	Physical	Backup
			Tampering	Physical	Physical Security
	Integrity	MiTM	Sybil Attack	Physical, MAC, Network	code attestation, radio resources testing, key pool
			Spoofing message tamper	Network	anti-spoofing software
		Malware	Injection	Application	
			Virus	Application	
			Worms	Application	

Table 3. Privacy threats in IoT

Threat	Impact	Attack	Type	Layer of Impact	Solution
Privacy	Confidentiality	MiTM	Eavesdropping	Network	Encryption
			Impersonation	Network	Encryption
			Sniffing	Network	Encryption
			Authroization	Application	Access Control
		Data Privacy	Data Leakage	Multiple	
			Re-identification	Multiple	data suppresion, generalization, noise addition
			Data tampering	Multiple	anonymization
			Identity Theft	Multiple	anonymization
		Others	Poodle	Transport	Use TLSv1.2
			Heartbleed	Transport	
			Freak	Transport	Turnoff export ciphersuit options in browser

Table 1. Security threats in IoT

IV. LITERATURE SURVEY

4.1 Machine Learning Algorithm Review Articles

Technology is making hackers more sophisticated, making attack prevention difficult. Resource-constrained IoT devices find defense harder. ML algorithms are employed to identify these assaults. ML is the capacity to learn from data and alter ML model output. Machines learn from their prior outcomes and improve using ML. ML algorithms have helped prevent security and privacy breaches. We explain these methods in the next subsections.

Restuccia et al. [1]employing ML techniques, we aimed to give a taxonomy of known vulnerabilities to IoT security and potential SDN mitigations of those dangers. Since gathering information from IoT devices is a primary function of any IoT system, they also proposed segmenting the data collecting procedure into three distinct phases: authentication of IoT devices, wireless networking of IoT devices, and data aggregation and validation. The paper provided a high-level summary of ML methods used to counteract security breaches, such as the application of Bayesian learning to identify cross-layer harmful assaults and the use of neural networks to evaluate the reliability of data. However, the report does not provide a thorough evaluation of the other ML algorithms.

Sharmeen et al. [2]intended to let developers of Industrial Internet of Things (IIoT) applications use APIs securely. The authors proposed training the ML model for malware detection with static, dynamic, and hybrid features. Using a dataset's performance metrics, features extraction method, features selection criteria, accuracy, and detection method, we conduct an in-depth evaluation of each feature class. A variety of detection strategies were evaluated for each feature set, however RF, SVM, KNN, J48, and NB were the most prevalent. Hybrid analysis, as concluded by allowed for a greater degree of freedom in deciding which static and dynamic characteristics to use, hence increasing detection precision. Unfortunately, the scope of this article cannot extend beyond a single use case (Android devices) and a single security issue (malware).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

Chaabouni et al. [3]focuses on network intrusion detection systems that make advantage of the Internet of Things as well. IoT design problems were discussed, including heterogeneity, mobility, trust and privacy, resource limits, connection, and data exchange, and presented in a layer-by-layer format (perception layer, network layer, application layer).

Traditional IoT security techniques were outlined, and the research concentrated on anomaly and hybrid network intrusion detection systems (ANIDS) for IoT devices. The authors of this article compared the design, detection methods, and experimental outcomes of classic NIDS with those of IoT systems. The research went on to show how the Learning-based NIDS for IoT may succeed where conventional IoT systems had failed. When everything was said and done, the best IoT NIDS concepts were compared with an eye toward ML techniques.

Xiao et al. [4] we looked at the privacy risks associated with MCS, where participants submit sensing reports of their surroundings to the MCS server and the information of interest is derived from those reports.

Participants and the MCS server both face serious privacy risks as a result of this information exchange. System vulnerabilities include advanced persistent threats, faked sensing assaults (in which false reports are sent to the server to lessen the sensing attempts), and privacy leaks (which is connected to user personal information) (causing privacy leakage over an extended period). The study recommended Deep Belief Networks (DBNs) and Deep Q-Networks (DQNs) for counter-measuring falsified sensing, as well as Deep Neural Networks (DNNs) and Convolutional Neural Networks (CNNs) for privacy protection. However, just a single application was considered for this evaluation (MCS)

V. MACHINE LEARNING

Machine learning, or deep learning (a term used interchangeably), is the method to artificial intelligence. In 1959, Arthur Samuel created the phrase "machine learning" to describe the ability of machines to learn without being given specific instructions. Without machine learning, AI can be built by hand, but it would need an enormous amount of labor, such as the creation of millions of lines of code with several rules and decision trees. Machine learning eliminates the need for such laborious human intervention by "training" an algorithm to improve itself over time. To the contrary, you are providing AI with massive volumes of data rather than code. For instance, Facebook use ML to identify key face traits of a video subject in real time. Furthermore, their ML platform is better able to adapt to new requirements due of the vast amount of data available. Using machine learning, organizations can more quickly react to customer emails, spot clouds in satellite imagery, and locate potentially habitable planets in the distant universe.

5.1 Understanding the Role of AI and ML in IoT

When combined, AI and ML will have a profound impact on the management and use of IoT gadgets. It's analogous to the connection between the mind and the rest of the body. The senses—sight, touch, and hearing—provide the body with information about its immediate environment, which may then be processed in the brain to provide rational choices.

The true difficulty is in finding a means to link disparate devices to a common infrastructure without compromising data or functionality. Envision a world in which all your Internet of Things gadgets could be managed from a single interface. With Tantiv4, you can take use of the advantages of both edge and cloud computing thanks to the company's own AI-based interactive platform.

VI. CONCLUSION

The Internet of Things (IoT) has improved human life by making it more convenient, stress-free, and pleasant. Challenges, such as those related to the security of IoT devices, have emerged as a result of these developments and the creation of smarter things. When faced with modern security threats, the tried-and-true procedures and resources of the past are useless.

When applied to improving the security of the Internet of Things (IoT), machine learning shows great promise. This study is a thorough, up-to-date assessment of the literature on the topic of the security and safety of the Internet of Things, including such topics as the IoT's design, specific security concerns, and potential entry points into the system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, December 2022
Impact Factor: 6.252

In addition, a thorough analysis of machine learning applications is provided. Finally, we highlight some of the problems, obstacles, and potential future research avenues that may be pursued in order to build a more secure Internet of Things.

REFERENCES

[1]. Rancesco Restuccia, Salvatore DrOro, and TommasoMelodia. 2018. Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking. *IEEE Internet of Things Journal* 1, 1 (2018), 1–14

[2]. Shaila Sharmeen, Shamsul Huda, Jemal H. Abawajy, Walaa Nagy Ismail, and Mohammad Mehedi Hassan. 2018. Malware Threats and Detection for Industrial Mobile-IoT Networks. *IEEE Access* 6 (2018), 15941–15957.

[3]. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Communications Surveys Tutorials* 21, 3 (third quarter 2019), 2671–2701.

[4]. Liang Xiao, Donghua Jiang, Dongjin Xu, and Ning An. 2018. Secure Mobile Crowd sensing with Deep Learning. *China Communications*15 (2018), 1–11. http://arxiv.org/abs/1801.07379

[5]. Elena Milosevic, MiroslawMalek, and Alberto Ferrante. 2016. A Friend or a Foe? Detecting Malware using Memoryand CPU Features. In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016)*, Vol. 4. 73–84.

[6]. Muhamad Erza Aminanto, Rakyong Choi, Harry Chandra Tanuwidjaja, Paul D. Yoo, and Kwangjo Kim. 2017. Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. IEEE Transactions on Information Forensics and Security 13, 3 (2017), 621–636.

[7]. Mandrita Banerjee, Junghee Lee, and Kim Kwang Raymond Choo. 2018. A blockchain future for internet of things security: a position paper. Digital Communications and Networks 4, 3 (2018), 149–160. https://@doi.org/10.1016/j.dcan.2017.10.006

[8]. I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock. 2018. Standardising a moving target: The development and evolution of IoT security standards. In Living in the Internet of Things: Cybersecurity of the IoT - 2018. 1–9

[9]. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys Tutorials 21, 3 (third quarter 2019), 2671–2701

[10]. Konstantinos Christidis and Michael Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things.IEEE Access 4 (2016), 2292–2303. http://ieeexplore.ieee.org/document/7467408/

[11]. Tim Dalgleish, J. Mark G.. Williams, Ann-Marie J. Golden, Nicola Perkins, Lisa Feldman Barrett, Phillip J.Barnard, Cecilia Au Yeung, Victoria Murphy, Rachael Elward, Kate Tchanturia, and Edward Watkins. 2018. The Blockchain-enabled Intelligent IoT Economy. (2018). https://www.forbes.com/sites/cognitiveworld/2018/10/04/the-blockchain-enabled-intelligent-iot-economy/#14b65de82a59