Comprehensive Survey Over Security and Protection Issues of IoT Devices

Muhammad Waqas[1], Muhammad Jawad Noonari[1], Hamza Altaf Khatri[1], Umair Saeed[1] and Rehan Ali[2]
[1]Department of Computer Science, Sindh Madressatul-Islam University Karachi, 74000, Pakistan
[2]Department of Computer Science, Dawood University of Engineering & Technology, Karachi, 74800, Pakistan.

E-mail:muhammad.waqaspn@gmail.com, jawadnoonari@gmail.com, hamzakhatri@gmail.com, umairsaeedmixit@gmail.com, eng.rehan75@yahoo.com

Corresponding Author: Muhammad Waqas, muhammad.waqaspn@gmail.com

Received: 26-06-2022; **Accepted:** 23-08-2022; **Published:** 29-08-2022

Abstract: The Internet of Things (IoT) technology has been involved nearly in each sector of daily life from home to industries level. It is another modern worldview pictured as a standard employer of interconnected machines. IoT technology brought easiness and increased the efficiency of communication between human and devices as compared to manual devices. Due to the increment in the usage of IoT devices in residential and commercial areas, these devices attracted the attackers for the security breaches. The main function of IoT security is to promise to provide the security and protection of private data of IoT users, data and devices and infrastructure. The end users are like a layman and do not have enough knowledge of these security holes that is why they are the easy target for the attackers. Various methods are acquainted with lift out and make use of IoT ideas. IoT technology is playing a critical role in every field like savvy properties and intelligent city areas, elevating safety concerns. This paper presents a review on security threats, the reason and order of these threats, and the preparations that had been given towards these IoT protection issues.

Index Terms: Internet of Things (IoT), IoT security, IoT gadgets, IoT security resolving issues.

1. Introduction

Internet of things (IoT) allow to the organization of interrelated actual electronic gadgets associated with the Internet or different electronic gadgets that can gather, offer and follow up on information without the involvement of any human or any intermediate collaboration between human and equipment. Scientists, Researchers, IT experts and IT enterprises created distinctive IoT gadgets and sensor-based devices. Fig.1 illustrates the use of IoT devices in every field of daily routine [1]. The term IoT had been proposed to exceptionally recognize the associated electronic gadgets utilizing radio-recurrence distinguishing proof [2]. Electronic gadgets, which are associated through IoT change on the basis of requirement in their sizes and shapes. A home automation system is one of the good real-life examples of IoT devices installation where electrical power, refrigerators, heaters, LED Screens, security cameras, and different electronic gadgets are associated at an IoT paradigm. Due to revolutionary headways, it has been now ended up practicable to interface domestic apparatuses, vehicles, even coronary heart screens, and others with the use of IoT. Electronic gadgets with implanted sensors are related at an IoT stage. The IoT technology is used to gather information from specific devices contemporary to generate statistical values, such an extent that it can pick what statistics is useful and what isn't.

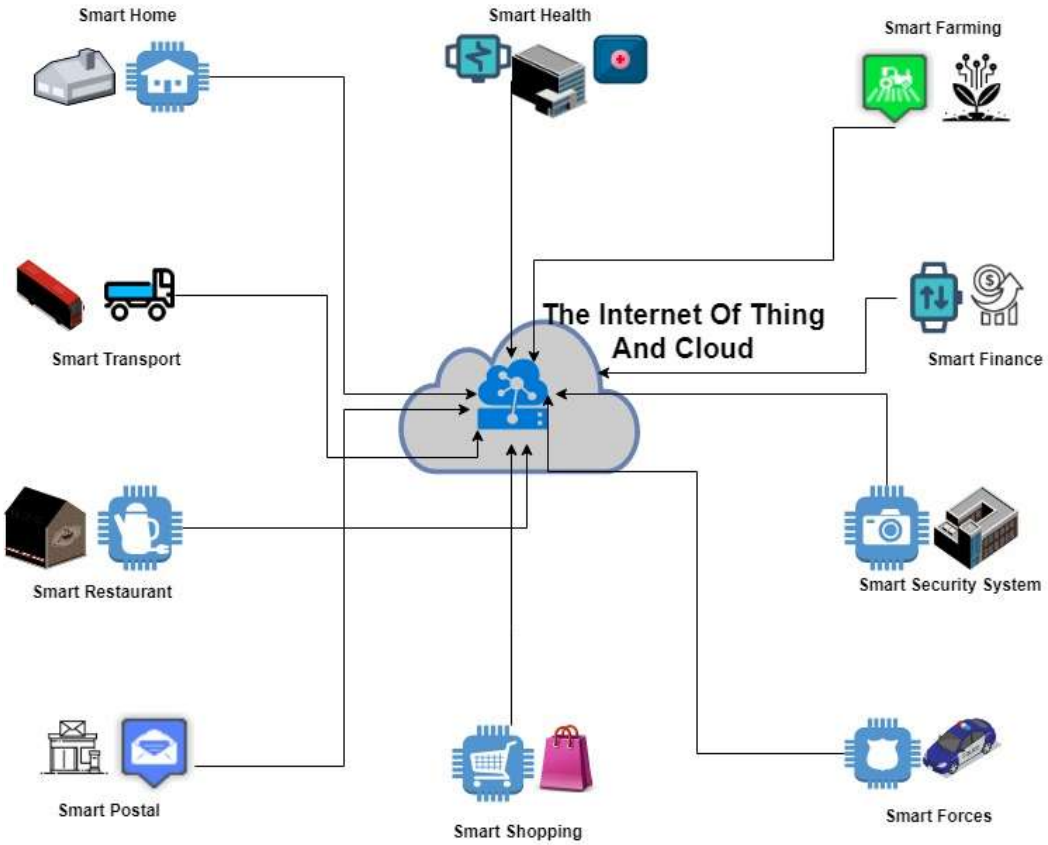

Figure 1. IoT application in daily life activities [1]

The savvy domestic concept relies upon on this headway of IoT where unique first-rate devices are placed in the residence are related with one IoT system and attached devices which provide ease to the customers. Clients can settle on flung recognizable article. WSN empowers correspondence amongst the electronic gadgets in or out of the organizations [2]. With the rising affiliation of IoT in more than a few fields of life, statistics safety breaks and goes after moreover increased [3-5]. This exploration plans to introduce a thorough evaluate in the house of IoT from the information safety viewpoint. Because of the quick improvement of IoT applications, many issues which were present in the IoT devices initially have been sorted out. This makes use of IoT more feasible and protected. This paper provides a comprehensive review on the threat and security challenges face by the IoT devices in present time and it also focuses on some of the past and future solutions in IoT security. While the vast use of IoT attracted the attention of many intruders and hackers. The massive usage of IoT devices created the security and safety issues in this field. For which, few examinations directed on IoT safety lately. It is essential for acquire the slicing side IoT safety trials when the preparations proposed in the direction of these smart devices. To lead a fantastic survey, an indispensable hunt string is formalized to accumulate considerable exploration in the paradigm of IoT security [6]. We zeroed in on more than a few distributions from well-known journals and gatherings.

This paper has been arranged in which section 2, describes the parts and layers in IoT devices. Section 3 examines the operatnig challenges mentioned in IoT design, characterization of IoT Security troubles as per the IoT layered design. It moreover offers the preparations available to these protection issues. Section 4 depicts the security and protection techniques for IoT. Section 5 provides the conclusion.

2. Parts and Layers in IOT Devices

The Internet of Things (IoT) has imagined becoming popular quickly due the expansion of correspondence innovation, the accessibility of the electronic gadgets, and computational frameworks. Subsequently, security from threats of IoT devices is a very crucial point to defend these devices from attacks as well as the organizations in which these IoT devices installed [7-8]. In any case, since system administration apparatuses is still somewhat new, security has not been thought of in the creation of these apparatuses. A few instances of existing IoT frameworks are self-driving

vehicles (SDVs) [9] for computerized vehicular frameworks, microgrids for appropriate energy asset frameworks, and Smart City Drones for reconnaissance frameworks. A microgrid framework addresses a genuine illustration of a hyperphysical framework. It interfaces generally disseminated energy assets (DER) together to give a far-reaching energy answer for a nearby geological locale. Be that as it may, a microgrid IoT framework actually depends on customary Supervisory Control and Data Acquisition (SCADA) [10].

Lightweight conventions for the electronic gadgets, may communicate with each other through the entry gate at the edge. Besides, wireless sensor networks (WSN) [11] uphold dynamic correspondence, which is normally consistently based totally on the 802.15.4 norm. Among the IEEE convention, the coordination of the physical and digital spaces really increments the openness to assaults. Digital assaults might focus on the SCADA administrative control and incapacitate the actual space, or the physical gadgets might be altered or compromised, influencing the administrative control framework. Then again, the robot market is moving rapidly to embrace computerization procedures and can be coordinate into putting out fires, police, shrewd city reconnaissance, and crisis reaction. As regions and residents depend on such a framework, it will become basic to keep the framework secure and solid.

Lately, it has been seen that scholastic examination to address the protection and security issues for IoT frameworks [7, 12]. The IoT design depends on a 3-level/layer framework which comprises of an insight/equipment layer, an organization/correspondence layer, and a layer of points of interaction/administration [12-13]. The components that make up an IoT framework are equipment/gadgets, correspondence/informing conventions, and points of interaction/administration. IoT devices contain the actuators and sensors in them, these are the main functioning components of the IoT environment. The special type of designed microprocessor is utilized at the physical layer is mainly designed by X.86, MIPS and ARM models. Preferably, designers ought to likewise integrate security techniques, which might incorporate a security chip or cryptographic code processor. The special type of operating system for IoT devices, on which these IoT devices normally operate on, is a Real Time Operating System (RTOS) [14], which incorporates a microkernel, equipment reflection layer, correspondence drivers, and capacities like cycle seclusion, application sandbox and secure boots.

For the proper working of the application of IoT devices at software layer, there are tools such as outsourcing drivers and libraries, cryptographic functions, and customized applications. Specifically, equipment choice is basic for getting the IoT gadgets. The worries with respect to the IoT equipment are validation capacities, which perform start to finish loading of the secure boot-stacking process, encryption of the outgoing traffic, during the updating of the IoT firmware the implementation of digital signatures, and straight forward exchanges. The following significant part of an IoT framework incorporates the correspondence and informing conventions. An organization of savvy items can convey straight forwardly to the Cloud by means of an entry way, through cloud administrations like Amazon Kinesis. Nonetheless, the significant idea of IoT is executing a Wireless Sensor Network (WSN) as the predominant correspondence innovation in the IoT. WSN has lightweight conventions for the electronic gadgets to communicate with each kind and with the entry way at the edge.

Besides, WSN upholds dynamic correspondence, which is consistently based on the 802.15.4 norm. Among the IEEE conventions, 802.15.4 is for Low Rate WPANs, which suits the necessities for an IoT framework [15]. Some blessings of this convention are its versatility and the way that it can be self-kept up with, the power consumption is very low, and has a low operating and maintenance cost. Nonetheless, 5G [16], 4G [16], WiFi [17], ZigBee [18] and Bluetooth [19] would additionally likewise be picked as the correspondence conventions, to swimsuit the requirements of the IoT processes. One more top size section in the IoT is the aggregator, which can be the passage for IoT engineering, for example, a Wi-Fi switch Passages give downstream availability to various "things". The Cloud services are one more favorable component in an IoT environment. Some well-known Cloud Service Providers (CSPs) are IBM, Google Cloud Platform, Microsoft Azure and Amazon Web Services [20].

The Cloud service providers offer different types of services for the IoT devices, including storage, information and data handling, data management and deal with privacy and security of the data. Furthermore, new support highlights are being presented by CSPs to Representees Stat Move (REST) correspondence conventions [21]. Consequently, the execution of IoT security relief ought to develop.

3. Operating Challenges to IOT Devices

IoT devices operate in three distinct ways. There are a variety of assessments about the extent of layers in IoT design, on the other hand it typically involves in three-layer engineering. Each of these three layers symbolizes the necessary thinking in the back of IoT. It is a proper layer, regularly referred to as the sensor layer. It is a critically analyzing job such as human perform different daily routine tasks with the help of their naturally built-in senses e.g., Nose for smell, ears for hearing, eyesight for view and so on. Edge devices have built in sensors and actuators, which

are used to interact and collaborate with other interconnected devices and the related environment as well. There is certainly not a solitary design that is considered as a norm or concurred by the specialists with the environment, distinguishing objects in the climate, gathering information, converting that information into helpful data, and passing it to the organization layer. The information from the vehicle layer and cycles that information into helpful data. The essential obligation of this layer is to eliminate the undesirable information and just store valuable data with the help of various models proposed overtime. There is certainly not a solitary design that is considered as a norm or concurred by the specialists. For that reason, only few models are accessible to date.

4. Security and Protection Techniques for IOT Devices

This portion of the paper elaborates available security threats, solutions and arrangements accessible to the featured IoT issues. The exact subtleties and examination of the accessible arrangements have been mentioned. Replay attacks [22] happened, when some interloper professed to be the first client of the framework and start communicating with different clients of the framework. It has been performed during the confirmation interaction. J. Srinivas et al [22] proposed a structure that identified what's more, mitigate the issue in the event that it exist. Discoveries included Universally Unique Identifier (UUI) for distinguishing objects extraordinarily, Timestamp, current season of the occasion and Battery Depletion Rate Monitor; to examine the battery utilization by the IoT parts involved. Replay Attack moderation is finished by just answering the solicitations with a legitimate gadget Id and MAC address [6]. Malware in IoT [4] expanded from 2015 and went past it. A notable firm Kaspersky announced 120000 malware assaults in 2018. They additionally explained the justification behind these assaults; the gadgets either had unpatched weaknesses or utilized default passwords. The answer for these malware's is principally connected with energy utilization patterns and OpCode.

M Waqas et al [1] used 11 machine learning algorithms over different 9 sensors devices datasets for the security and performance of the models for the detection of Botnet attack in intrusion detection system and calculated the 99% detection accuracy. D.E. Kouicem et al [5] presented a structure for the detection of malware in IoT devices with help of a deep machine learning model. For the completion and better result of their research work, they pre-processed the data and then extracted the different features and Opcode and afterward they have selected the best 10 Opcodes designated by the aggressors. The precision of location is generally better compared to other people [5]. Domain Name System (DNS) fills in as the interpreter for the gadgets able to do associating with the IoT system for different administrations. IoT, as we probably are aware, has short storage capacity and power handling, so models for the security of DNS can't be executed. It presents dangers like Man-In-The-Middle attacks and Cache Poisoning in DNS [23-25].

Jian Zhang et al [26] provided a review over the security models of IoT at each level. In their paper, they highlighted different security threats like physical, network and information data threats. Furthermore, they provided the present and future solution for IoT threats and intrusion detection. K. Chen et al [6] designed an electronic device for the monitoring of the traffic regularly, by the use of this device malicious logging, threats and traffic can be monitor. The presented techniques tell suspicious traffic in view of the framework director characterized decide and packet measures that are configurable. IoT devices have limited storage and small power to process the tasks. For this reason, just lightweight crypto frameworks are utilized in this stage that stand out for the assailants and dealing with the attacks and threats since these arrangements are not fit well [4, 27]. F. Wu et al [28] provided a memory proficient multi-key age plot that gets data transmission between IoT gadgets and the cloud.

Furthermore, Table 1 defines the security threats and challenges face by the IoT devices in different aspects. Table 2 describes the available techniques for the protection of IoT devices.

Table 1. Security Threats and Challenges in IoT Devices

Threats	***Features***	***Challenges***
Threats face by IoT devices	Resource-constraint	Loss of Identity, Nodes Destruction and Tamper with Label content
Threats in Communication between Networks	Heterogeneity, Manageability and controllability, Rules and Protocols	DDoS attack, Privacy breach, Side Channel attack, IP spoofing, Vulnerabilities in Control Nodes and Vulnerabilities in Protocols
Threats for Data Information	Availability, Accessibility, Confidentiality and Integrity	Modification in data and Replay Attack

Table 2. Available Protection Techniques for IoT Devices

References	***Research Work***	***Protection Techniques***
[29-30]	IoT devices privacy, security protection and Access control	Access control methods: network and permission access control, security and privacy control at directory level, attribute and server control, Independent, mandatory, and role-based access control. IoT devices privacy issues: Physical device security, encryption, and smart tags.
[31-34]	Solution of traffic detection and Intrusion detection	Intrusion detection methods: Anomaly, specification, misuse, mixed detection methods. Intrusion detection systems: Different Signature based, network based and machine learning algorithms-based intrusion detection systems.

5. CONCLUSION

In this paper, the motivation behind this study has been achieved by giving a sufficient outline of the examination patterns in IoT security between 2016 until 2022 and the applicable devices and test systems. The main target of this research article is to express the all the possible security threats revealed in IoT devices. The different types and methods of these security threats are likewise presented. In the wake of gathering that multitude of detailed issues, one more examination was directed to comprehend the number of arrangements that were accessible to handle those security challenges. Each of the arrangement was accumulated and introduced mainly given, arrangements were tending to a solitary security issue. In spite of the fact that organization, the exploration from trustworthy distributers have been audited and ordered for simple reference from new scientists. Future research work of this article is to design a hybrid model by the use of different algorithms and apply this model on available datasets to determine the accuracy and performance of the model for anomaly detection on an IoT security system. Channel often give direct associations with the specific things. Along these lines by expounding on the encounters on web journals as a way to organizations can find out about what they have done right and what they need to develop, increase the proportion in the internet security have come to they go online by implication drawing in the organizations.

References

[1] Waqas, Muhammad, Kamlesh Kumar, Asif Ali Laghari, Umair Saeed, Muhammad Malook Rind, Aftab Ahmed Shaikh, Fahad Hussain, Athaul Rai, And Abdul Qayoom Qazi. "Botnet Attack Detection In Internet Of Things Devices Over Cloud Environment Via Machine Learning." Concurrency And Computation: Practice And Experience 34, No. 4 (2022): E6662.

[2] Sha, Kewei, Wei Wei, T. Andrew Yang, Zhiwei Wang, And Weisong Shi. "On Security Challenges And Open Issues In Internet Of Things." Future Generation Computer Systems 83 (2018): 326-337.

[3] Sfar, Arbia Riahi, Enrico Natalizio, Yacine Challal, And Zied Chtourou. "A Roadmap For Security Challenges In The Internet Of Things." Digital Communications And Networks 4, No. 2 (2018): 118-137.

[4] Chasaki, Danai, And Christopher Mansour. "Security Challenges In The Internet Of Things." *International Journal Of Space-Based And Situated Computing* 5, No. 3 (2015): 141-149.

[5] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet Of Things Security: A Top– Down Survey, Comput. Networks 141 (2018) 199–221.

[6] Chen, Kejun, Shuai Zhang, Zhikun Li, Yi Zhang, Qingxu Deng, Sandip Ray, And Yier Jin. "Internet-Of-Things Security And Vulnerabilities: Taxonomy, Challenges, And Practice." Journal Of Hardware And Systems Security 2 (2018): 97-110.

[7] Yang, Yuchen, Longfei Wu, Guisheng Yin, Lijie Li, And Hongbin Zhao. "A Survey On Security And Privacy Issues In Internet-Of-Things." Ieee Internet Of Things Journal 4, No. 5 (2017): 1250-1258.

[8] Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, And Wei Zhao. "A Survey On Internet Of Things: Architecture, Enabling Technologies, Security And Privacy, And Applications." Ieee Internet Of Things Journal 4, No. 5 (2017): 1125-1142.

[9] Lliu, Peng, Run Yang, And Zhigang Xu. "How Safe Is Safe Enough For Self-Driving Vehicles?." Risk Analysis 39, No. 2 (2019): 315-325.

[10] Upadhyay, Darshana, And Srinivas Sampalli. "Scada (Supervisory Control And Data Acquisition) Systems: Vulnerability Assessment And Security Recommendations." Computers & Security 89 (2020): 101666.

[11] Song, Xudan, Jing Wang, Sijia Liu, Xiaohan Cui, And Rong-Rong Yin. "Cascading Failure Mitigation Strategy For Urban Road Traffic Networks." In Wireless Sensor Networks: 15th China Conference, Cwsn 2021, Guilin, China, October 22–25, 2021, Revised Selected Papers 15, Pp. 170-180. Springer Singapore, 2021.

[12] Tewari, Aakanksha, And Brij B. Gupta. "Security, Privacy And Trust Of Different Layers In Internet-Of-Things (Iots) Framework." Future Generation Computer Systems 108 (2020): 909-920.

[13] Kumar, Sanjeev, And Sukhvinder Singh Deora. "Security Challenges And Issues In Iot." In 2021 6th International Conference On Signal Processing, Computing And Control (Ispcc), Pp. 171-175. Ieee, 2021.

[14] Baccelli, Emmanuel, Cenk Gündoğan, Oliver Hahm, Peter Kietzmann, Martine S. Lenders, Hauke Petersen, Kaspar Schleiser, Thomas C. Schmidt, And Matthias Wählisch. "Riot: An Open Source Operating System For Low-End Embedded Devices In The Iot." Ieee Internet Of Things Journal 5, No. 6 (2018): 4428-4440.

[15] Mubashar, Rehman, Muhammad Abu Bakar Siddique, Ateeq Ur Rehman, Adeel Asad, And Asad Rasool. "Comparative Performance Analysis Of Short-Range Wireless Protocols For Wireless Personal Area Network." Iran Journal Of Computer Science 4 (2021): 201-210.

[16] Giust, Fabio, Gianluca Verin, Kiril Antevski, Joey Chou, Yonggang Fang, Walter Featherstone, Francisco Fontes Et Al. "Mec Deployments In 4g And Evolution Towards 5g." Etsi White Paper 24, No. 2018 (2018): 1-24.

[17] Liu, Fen, Jing Liu, Yuqing Yin, Wenhan Wang, Donghai Hu, Pengpeng Chen, And Qiang Niu. "Survey On Wifi-Based Indoor Positioning Techniques." Iet Communications 14, No. 9 (2020): 1372-1383.

[18] Khanji, Salam, Farkhund Iqbal, And Patrick Hung. "Zigbee Security Vulnerabilities: Exploration And Evaluating." In 2019 10th International Conference On Information And Communication Systems (Icics), Pp. 52-57. Ieee, 2019.

[19] Bluetooth, S. I. G. "Bluetooth Technology." (2020).

[20] Ucuz, Derya. "Comparison Of The Iot Platform Vendors, Microsoft Azure, Amazon Web Services, And Google Cloud, From Users' Perspectives." In 2020 8th International Symposium On Digital Forensics And Security (Isdfs), Pp. 1-4. Ieee, 2020.

[21] Tatyasaheb, Dhokane Nilima, And Binod Kumar. "Implementation And Comparison Of Mqtt Protocol To Check The Drawbacks For Future Enhancement." In 2021 International Conference On Computing, Communication And Green Engineering (Ccge), Pp. 1-6. Ieee, 2021.

[22] Srinivas, Jangirala, Sourav Mukhopadhyay, And Dheerendra Mishra. "Secure And Efficient User Authentication Scheme For Multi-Gateway Wireless Sensor Networks." Ad Hoc Networks 54 (2017): 147-169.

[23] Shinzaki, Takashi, Ikuya Morikawa, Yuji Yamaoka, And Yumi Sakemi. "Iot Security For Utilization Of Big Data: Mutual Authentication Technology And Anonymization Technology For Positional Data." Fujitsu Sci. Tech. J 52, No. 4 (2016): 52-60.

[24] M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, Authentication Protocols For Internet Of Things: A Comprehensive Survey, Security And Communication Networks 2017 (2017) 1–41.

[25] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K.R. Choo, A Robust And Energy Efficient Authentication Protocol For Industrial Internet Of Things, Ieee Internet Of Things Journal 5 (3) (2018) 1606–1615.

[26] Zhang, Jian, Huaijian Chen, Liangyi Gong, Jing Cao, And Zhaojun Gu. "The Current Research Of Iot Security." In 2019 Ieee Fourth International Conference On Data Science In Cyberspace (Dsc), Pp. 346-353. Ieee, 2019.

[27] Chernyshev, Maxim, Zubair Baig, Oladayo Bello, And Sherali Zeadally. "Internet Of Things (Iot): Research, Simulators, And Testbeds." Ieee Internet Of Things Journal 5, No. 3 (2017): 1637-1647.

[28] Wu, Fan, Xiong Li, Lili Xu, Saru Kumari, Marimuthu Karuppiah, And Jian Shen. "A Lightweight And Privacy-Preserving Mutual Authentication Scheme For Wearable Devices Assisted By Cloud Server." Computers & Electrical Engineering 63 (2017): 168-181.

[29] Lin, Li, Ting-Ting Liu, Shuang Li, Chathura M. Sarathchandra Magurawalage, And Shan-Shan Tu. "Priguarder: A Privacy-Aware Access Control Approach Based On Attribute Fuzzy Grouping In Cloud Environments." Ieee Access 6 (2017): 1882-1893.

[30] Hänel, Thomas, Alexander Bothe, René Helmke, Christoph Gericke, And Nils Aschenbruck. "Adjustable Security For Rfid-Equipped Iot Devices." In 2017 Ieee International Conference On Rfid Technology & Application (Rfid-Ta), Pp. 208-213. Ieee, 2017.

[31] Rathore, Shailendra, And Jong Hyuk Park. "Semi-Supervised Learning Based Distributed Attack Detection Framework For Iot." Applied Soft Computing 72 (2018): 79-89.

[32] Lee, Po-Yen, Chia-Mu Yu, Tooska Dargahi, Mauro Conti, And Giuseppe Bianchi. "Mdsclone: Multidimensional Scaling Aided Clone Detection In Internet Of Things." Ieee Transactions On Information Forensics And Security 13, No. 8 (2018): 2031-2046.

[33] Anjum, Farooq, Dhanant Subhadrabandhu, Saswati Sarkar, And Rahul Shetty. "On Optimal Placement Of Intrusion Detection Modules In Sensor Networks." In First International Conference On Broadband Networks, Pp. 690-699. Ieee, 2004.

[34] Onat, Ilker, And Ali Miri. "An Intrusion Detection System For Wireless Sensor Networks." In Wimob'2005), Ieee International Conference On Wireless And Mobile Computing, Networking And Communications, 2005., Vol. 3, Pp. 253-259. Ieee, 2005.

