IoT Insider Attack - Survey

Morshed U. Chowdhury[1](✉), Robin Doss[1], Biplob Ray[2], Sutharshan Rajasegarar[1], and Sujan Chowdhury[2]

[1] Center for Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, Australia
{morshed.chowdhury,robin.doss, suthershan.rajasegarar}@deakin.edu.au

[2] Centre for Intelligent Systems (CIS), Central Queensland University, Rockhampton, Australia
{b.ray,s.chowdhury2}@cqu.edu.au

Abstract. The “Internet of things” (IoT) creating a perfect storm in the smart world. Due to the availability of internet and capabilities of devices, sensors-based technologies becoming popular day by day. It now opens the opportunities for overcoming many new challenges. Any device with on/off capability connecting through the internet via sensor can be an IoT device which includes a coffee machine, light, hand watch, headphones, washing machine, mobile phones, car, CCTV camera and so on. Simply we can say connecting things to people via the internet and controlling remotely is the great advantage of IoT. In our daily life, the IoT is widely used which includes transportation, health, education, security and so on. Imagine how IoT can make our life easier, based on your set alarm when you wake up if it can notify your coffee machine to prepare coffee for you that will save you time. Despite those advantages, the IoT based system is not free from vulnerabilities. Different types of attacks make the system vulnerable and tried to exploit the system and creating obstacles from its growth. Here we will explore IoT attacks and the relevant technologies associated along with machine learning strategies that exist to overcome those obstacles.

Keywords: IoT · Insider attack · Mitigation technique · IoT application · Machine learning

1 Introduction

The Internet of Things (IoT) can act in three different ways, firstly, collecting information and sending it to the appropriate location, secondly, acting on collected information in an intelligent way and finally doing both automatically. For example, sensors like temperature, weather, light, moisture, air quality sensors can automatically collect information from the environment and make more intelligent decisions like watering land and send information when crops need to be cut. The applications of IoT have grown exponentially in a short period of time over the utility industry as well. Now a day’s smart grids for electricity, water and gas dominated by IoT. These varieties of use cases enhanced customer service and at the same time increase the overall value of a business. Beyond

D.-J. Deng et al. (Eds.): SGIoT 2019, LNICST 324, pp. 28–41, 2020.
https://doi.org/10.1007/978-3-030-49610-4_3

this, we can apply IoT technology for smart health initiatives by monitoring heart rate of an individual and alert nearby hospital or relatives in case of any emergency. It can be applicable in automobile industry to check the tire pressure using sensors and alert the driver if the tire pressure goes below limit. Thus, IoT adding value to the business and change the way of business operations. Investors need to change the ways of their business for the benefits of their organizations.

The main goal of IoT can be expressed as the following ways:

- Improve overall business experience
- Save money and time
- Improve the productivity of the employees
- Help investors for taking quick decisions
- Improve customer experience
- Generate more profit
- Keep the business model up to date with modern technologies

Because of the benefits of IoT technologies, it expands in numerous sectors like industry, individual and government which cover all areas of our life. Nowadays individual can control their home appliances like heating, lighting and electronic devices via smartphones and other internet accessible devices.

Not only controlling home but also wearing smartwatch as well as other wearable sensors is the most common fashion among the people with different ages. Those wearable sensors can collect and analyze data and give useful feedback on individual health which makes life easier and more comfortable. In case of emergency with the help of other sensors can respond quickly to provide an optimized route by tracking construction works or any other emergency work on the route. The IoT makes a significant contributions in health sector which includes real time health monitoring for patients and give instant results by analyzing and predicting possible problems. Sensors also can be used for inventory management and order automatically if stock reached a specific threshold.

Because of on growing growth of human being crises on electricity is one of the biggest issues all over the world. Using the advancement of sensors in IoT systems, the temperature can be adjusted by counting the number of people in the building as well as in the room. Automatically shutting down the lights and air conditioner if there are no occupants and control the temperature accordingly also one of the biggest achievements in the area of IoT. Not only in our daily life but also in the agriculture sector lots of improvement has been done and some are ongoing. Smart farming can monitor temperature, soil moisture, predicting rain, humidity level to do the watering and fertilizing the land. Sensors can predict the time of irrigating and can automatically pick up the selected crops from the land. The same technique can be applied to control the streetlight in a smart city. Sensors also can be used to monitor environmental concerns in terms of heavy traffic.

As illustrated in Fig. 1, the IoT is the center of our evolving smart world where automation, connectivity and productivity are not confined within a specific silo. The connectivity between objects, individual and computing devices from diverse silos are working together for smarter future in every steps of our life.

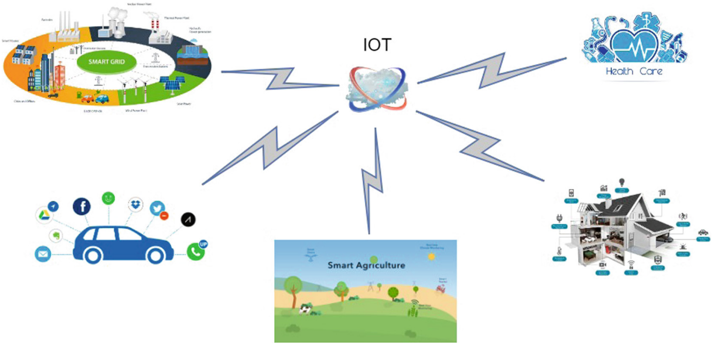

Fig. 1. IOT application scenario

Beyond the above-mentioned advantages, security and privacy is a great concern in IoT. As billions of sensors connect over the internet to collect and support the technologies it involves billions of data point which need to be secured to avoid data manipulation. As many people will try to take advantage by manipulating the data and make the system vulnerable for their own benefit, therefore, IoT security is one of the important focus research areas in the smart world.

The 2016 Dyn cyberattack is one of the biggest DDoS attack in IoT which makes most of the DNS (domain name server) vulnerable. This impact a large number of internet accessible devices which includes printer, baby monitor, security cameras and so on. The attack is known as Mirai botnet attack which is a malicious program which can replicate itself by exploiting poorly secured IoT devices and gain access by a central server. A manufacturer who didn't update their IoT product periodically became insecure hence prone to attacks.

As sensors are holding personal information like name, ages, mobile number, addresses even social network account therefore hackers can compromise these sensors and sale to relevant agencies. Not only hackers but also other risk factors like natural disasters, electricity, infrastructure also needs to be considered to make the overall system secure.

This paper will focus on the IoT attacks and what are the security mechanism taken so far to stop those known attacks. This research will also try to highlight the gaps and possible areas of improvement within the existing techniques.

2 Survey on IoT Attacks

In this section, we will discuss attacks based on layers architecture of IoT presented in Fig. 2. It is very important to understand the attack layers and types of attacks happen in each layer then it will be helpful to identify the causes. As illustrated in Fig. 2, we have presented the IoT network in four main layers where perception and sensing layers are accommodating most of the revolving IoT technologies. For example, Routing Protocol for Low-Power and Lossy Networks (RPL), RFID (Radio Frequency Identification) and WSN (Wireless Sensor Networks) are the technologies used by IoT which belong to the last two layers as mentioned previously.

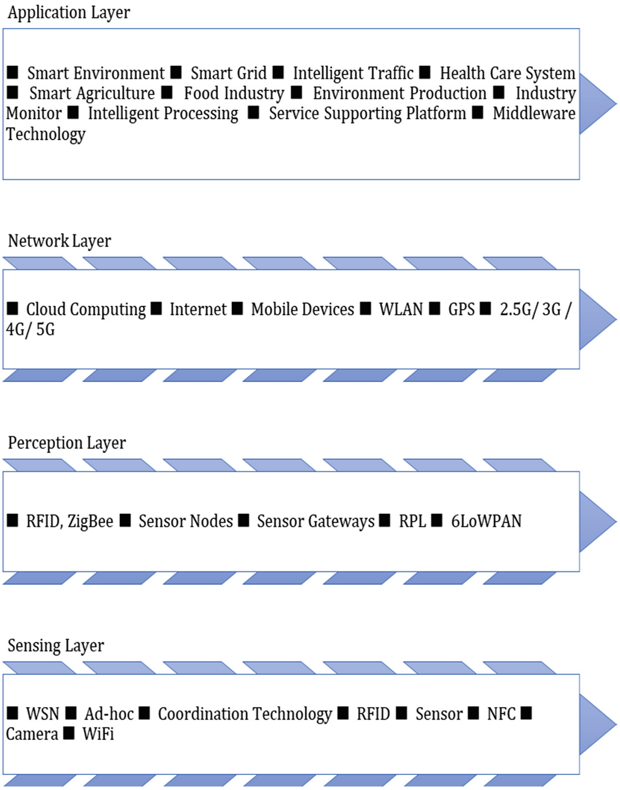
Application Layer
■ Smart Environment ■ Smart Grid ■ Intelligent Traffic ■ Health Care System ■ Smart Agriculture ■ Food Industry ■ Environment Production ■ Industry Monitor ■ Intelligent Processing ■ Service Supporting Platform ■ Middleware Technology
Network Layer
■ Cloud Computing ■ Internet ■ Mobile Devices ■ WLAN ■ GPS ■ 2.5G/ 3G / 4G/ 5G
Perception Layer
■ RFID, ZigBee ■ Sensor Nodes ■ Sensor Gateways ■ RPL ■ 6LoWPAN
Sensing Layer
■ WSN ■ Ad-hoc ■ Coordination Technology ■ RFID ■ Sensor ■ NFC ■ Camera ■ WiFi

Fig. 2. IoT architecture

In next sub-section, we have presented attacks taxonomy based on our detail analysis of exiting literature.

2.1 IoT Attack Taxonomy

The attack happens at different levels based on the weakness and depends on the techniques of the security attacks. We start by categorizing of different IoT attacks and countermeasures in Table 1 which also presented the link of different protocols with the categories. As we can see in Table 1, the IoT attacks can be classified based on targeted technologies, nature of intrusion as well as penetration vicinity like from inside or outside. It might be a hardware or software attack. But most of the time it is software-based attack and there is also a possibility of physical or natural disaster-based attack.

In Fig. 3, we have presented the IoT attack taxonomy based on the existing attacks reported in the literature and in Table 1. The Fig. 3 presents a clearer IoT taxonomy which demonstrated that existing IoT attacks explored various IoT technologies by inside and outside intruders who are targeting to compromise mainly three areas: information, operation and access level of devices.

Table 1. Classification of attacks and countermeasures detail

Attacks	Description	Protocols involved	Countermeasures	Category
Low end class	Low power device that are constrained in terms of resources which are designed for basic sensing. Examples are OpenMote-B and Atmel SAMR21 Xplained-Pro (Ojo et al. 2018)	UART, SPI, I2C	Deep-Learning-Driven Intrusion Detection Techniques (Thamilarasu and Chawla 2019)	Device property-based attack
High end class	Powerful device can be accessible through internet from anywhere. Examples are Raspberry Pi (Ojo et al. 2018)	TCP-IP, MQTT, CoAP, BLE	Machine Learning based Intrusion Detection (Yair Meidan 2017)	Device property-based attack
Insider attack	Compromise security by a person or by code itself with authorized system access (Kammüller et al. 2016)	Bluetooth, RFID, Zeebee	RFID authentication and encryption techniques	Location based attack
Outsider attack	If security comprise by outsider who can gain access protected information (Jang-Jaccard and Nepal 2014)	IP, TCP or DNS	Secure channel and do network authentication	Location based attack
Physical	Manipulating the device at physical layer to prevent sensors from detecting general risks such as fire, flood or unexpected motion (Ali and Awad 2018)	Man in the middle (MITM)	Secure the physical locations of installed devices	Strategy
Logical	Communication channel interrupted by external attack without damaging physical device (Ali and Awad 2018)	COAP, XAMP, HTTP	Security protocols based on AES	Strategy
Passive	When an attacker doesn't manipulate any information but can read all the traffic is known as passive attack. Attackers always looking for open ports and vulnerabilities of a system (Arış et al. 2018)	RPL	Automata Based Intrusion Detection Method	Access level
Active	When an attacker cause damage or manipulate information when gain access is known as active attack. (Nurse et al. 2015)	RPL	Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders (Meidan et al. 2018)	Access Level

(*continued*)

Table 1. (*continued*)

Attacks	Description	Protocols involved	Countermeasures	Category
Disruption	When availability of IOT device interrupted by attackers then it known as protocol disruption	RPL	Classification based detection (Zhang et al. 2014)	Protocol Based
Deviation	When attacker writes malicious code on the IOT system is known as deviation from the protocol. Examples like DDOS attack (Mustapha and Alghamdi 2018)	Application and Network Protocol	Rule based detection	Protocol Based
Interception	Also known as man in the middle attack where the attacker secretly read all the message and intercept the message	MTTM	SWAP: Mitigating XSS Attacks using a Reverse Proxy (Wurzinger et al. 2009)	Information Damage Level
Fabrication	By fabricating information in IOT device attacker damage the normal architecture of the system. Example like blackhole attack	RPL	Mitigation of black hole attack (Ahmed and Ko 2016)	Information Damage Level
Interruption	When a fake message is inserted into the IOT network by an intruder and gain control is known as interruption. Examples of this attack like unwanted shut down of IOT device	Network protocol	Software-Defined Internet of Things Framework (Yin et al. 2018)	Information Damage Level
Eavesdropping	Eavesdropping occurs when attacker will be able to install traffic monitoring system within the IOT device	Network protocol	A hybrid prevention method for eavesdropping attack by link spoofing (Tri-Hai Nguyen, 2017)	Information Damage Level
User	If a authenticate user explode security credential, make the device accessible	N/A	Logging user activities	Host Based
Hardware	Hardware tempering is another way of attack IOT device	N/A	Securing the hardware	Host Based
Software	Software within the IOT device if not updated periodically and if there is bug in the software can create damage in the overall IOT system	N/A	Updating the software	Host Based

(*continued*)

Table 1. (*continued*)

Attacks	Description	Protocols involved	Countermeasures	Category
Link	By doing repetitive collision and transmitting same frequency to the IOT devices simultaneously can create the attack	RPL	Link-layer metric as a parameter in the selection of the default route (Wallgren et al. 2013a)	Communication Stack Protocol (CSP)
Network	By creating loop in the routing table or by duplicating the node in the network creates the attack	RPL		CSP
Transport	Like DDOS and hello flood attack	RPL		CSP
Application	Sending malicious or fishing attack	RPL		CSP

ZigBee is a popular wireless communication technology for sensor communication. To get a further understanding of IoT device-based attacks, in Table 2, we have illustrated attacks under device based technologies. As we can see from Table 2, although there are a large number of existing attacks based on Wi-Fi communication technology, the ZigBee based attacks are on the rise due to its popularity in sensor communication.

2.2 IoT Routing Attacks

To further explore routing attacks in IoT, this article has presented existing attacks in RPL (Routing Protocol for Low-Power and Lossy Networks) based IoT networks in Table 3. The RPL is a popular routing protocol for sensor networks in IoT. As presented in Table 3, attacks are ground in three main categories based on their objectives. In the resource category, the attacks aim to compromise network resources using direct and indirect techniques which ultimately cause DoS attack. The topology of the sensor networks is dynamic which exploited by many attacks listed in the topology category. Finally, the attacks in traffic category eavesdrop sensors traffic over the insecure wireless network to identify vulnerabilities. As RPL works with low power and lossy network, it is difficult to find a full proof adaptive countermeasure as presented in the countermeasure section of Table 3 which shows most of the existing countermeasures are attack detection techniques.

2.3 RFID Attacks

RFID is an integral part of IoT technology like sensory tags due to its unique identification capability over the wireless medium. RFID tags are two types – active and passive and attack happens in both types. Despite the advantage of RFID readers security of the device gets compromised due to the limitation of RFID hardware. There are many attacks exist in RFID network which could be an easy entry point to the IoT network. In Fig. 4,

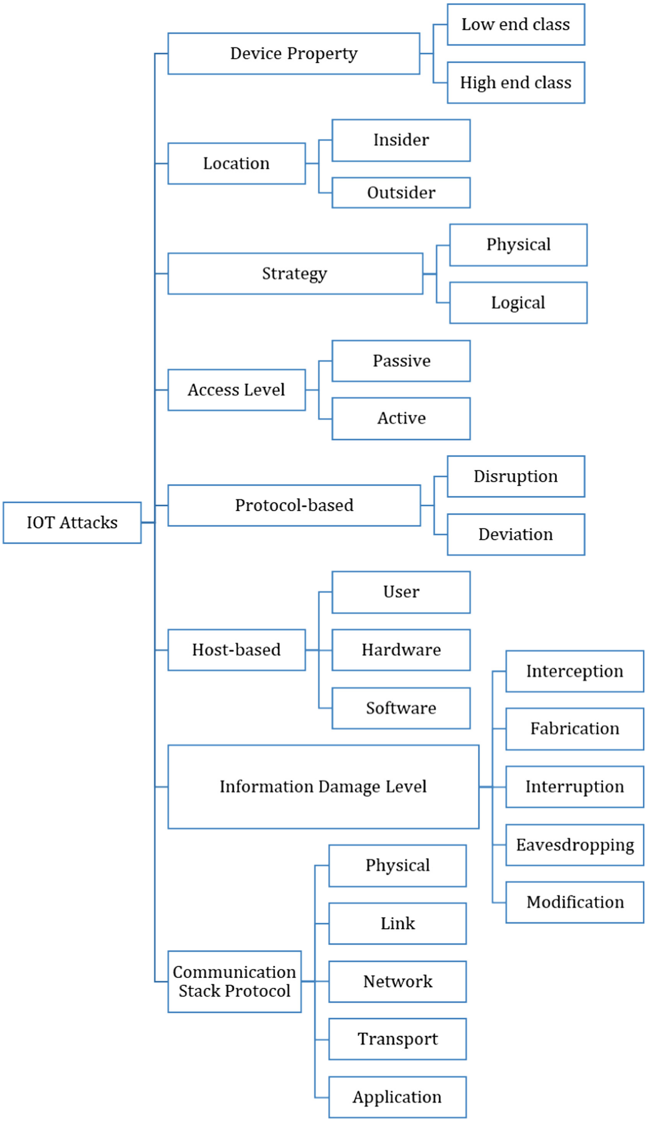

Fig. 3. IoT attack taxonomy

we have presented the taxonomy of existing RFID attacks which are categorized based layers of IoT network detailed in Fig. 1.

There are many lightweight techniques proposed by researchers in RFID tags and in readers to counter these RFID attacks detailed in Fig. 4. For example, lightweight sanitization technique (Ray et al. 2011 and Xiao et al. 2016), authentication techniques (Ahemd et al. 2017) and stenography (Ray et al. 2013) are some examples. As mentioned earlier, the virus can spread through RFID tags (Li et al. 2012) to the IoT networks. If we

Table 2. Device based attacks

Attacks	Descriptions	Protocols involved	Countermeasures	Types of attacks
Bluetooth Based Attack	The attack happens through Bluetooth and makes the IOT devices vulnerable	Bluetooth Protocol	Update software and put the device into non-discoverable mode or offline can mitigate the issue (Be-Nazir et al. 2012)	Bluesnarfing, BlueBugging, Bluejacking
Denial of Service	Flood of incoming message which will slow down the network or crush the overall system	Network Protocol	Using access control list and do blacklist suspicious devices (Liang et al. 2016)	Interception, Hijacking, Spoofing
Wifi Based Attack	As most of the modern IOT device accessible through WiFi intruders target WiFi and create damage	WEP Protocol	AES and RC4-based SSL (TLS) (Stubblefield et al. 2002)	Google Replay Attack, FMS Attack and so on
ZigBee based Attack	Most of the Zigbee device operate without using any encryption and therefore vulnerable for attack	ZigBee Protocol	Pre install network key and do a counter mechanism can stop some attack (Dowling et al. 2017), (Olawumi et al. 2014)	Sniffing and Replay Attack

compare types of security versus communication channels, we found encryption is weak in RFID. While authentication and authorization are fair for RFID, but sensor gateway and sensor nodes are strong in the authentication.

3 IoT Attacks and Future Research

Uses of IoT devices is increasing day by day. Recent research shows 20 billion IoT devices up-and-running so far. The number will be enormously increase as the 5G mobile network will dominate within few years which will connect more and more IoT devices. This large pool of internet connected devices will increase our dependency on the IoT network which will bring new vulnerabilities in light. The Mirai Botnet attack (Abdur Razzaq et al. 2017) might cause more damage and make it easy for bad guys to cause

Table 3. RPL Attack

Attack		Descriptions	Protocols involved	Countermeasures	Types of attacks
Resources	Direct Attack	Attackers directly exhaust the resources	RPL, User Datagram Protocol (UDP), Constrained Application Protocol (CoAP)	Intrusion detection mechanism with a lightweight heartbeat protocol (Wallgren et al. 2013a)	Flooding, Routing table overload
	Indirect Attack	Attacks happened from another malicious node	RPL, User Datagram Protocol (UDP), Constrained Application Protocol (CoAP)	Data path validation mechanism (Mangelkar et al. 2017), RPL loop detection and avoidance mechanisms (Kamble et al. 2017)	Increase rank attack, DAG inconsistency, Version attack
Topology	Sub optimization	Manipulate the routing table	TinyAODV Protocol, MintRoute Protocol	SVELTE (Raza et al. 2013), Rank verification, Parent fail-over, Geographical data, Merkel trees	Routing table falsification, Sinkhole, Wormhole, RI play, Worst parent
	Isolation	Isolating node from the actual communication in the network	AODV Protocol	Monitoring of counters	Blackhole, DAO Inconsistency
Traffic	Eavesdropping	Doing eavesdropping activities by deploying attacker node	HTTP, TELNET, FTP, POP, SNMP	Encryption	Traffic analysis, Sniffing
	Misappropriation	Discovering the topology of the network through malicious activity	Demand Source Routing (DSR), Optimized Link State Routing (OLSR), Zonal Routing Protocol (ZRP)	VeRA (Dvir et al. 2011), TRAIL (Landsmann et al. 2013)	Decreased rank attack, Identity attack

global damage. Now, most people use wearable devices which could be potentially affected by IoT attacks. The automated DevOps testing device from a less professional vendor might create security risk (Zhou et al. 2019). Furthermore, the shadow IT resource and IT professionals within the organization might be a serious concern for IoT networks.

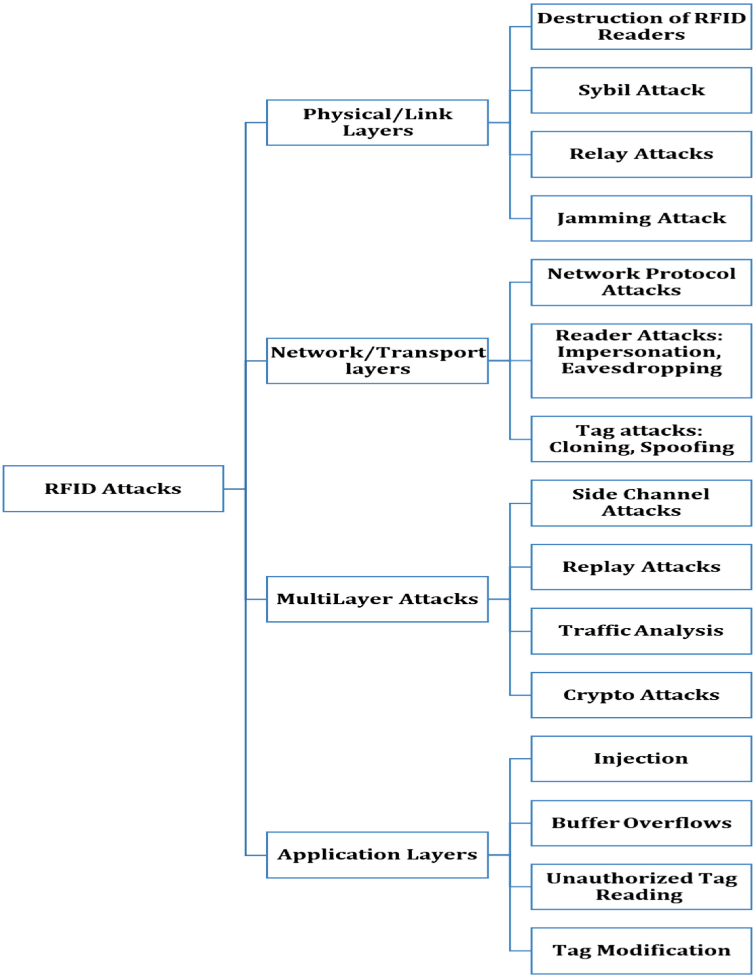

Fig. 4. RFID Attacks

Outdated hardware might be the biggest security challenge and automated identification of these weak devices will be one of the future research challenges. Although the growth of big data is not a big problem yet but as time pass by bigdata will be a serious concern due to gowning difficulties of the management and analysis of the dataset. Due to so much personal data collected by big companies via IoT, the security breaches will create a great damage for consumers. So, securing those personal data and create a technique of automatically destroying those data will be a future research direction for IoT security. The adaptive security techniques will be more effective to protect IoT network, therefore, a great deal of future research on IoT security will find an appropriate adaptive security that can learn from the live network and implement countermeasure thereafter.

4 Conclusion

IoT will be the future. Despite some security challenges, the IoT will dominate in every place which will cover from home to industry. This paper tries to highlight all the current attacks and known security issues which is already mitigated by different techniques. If the security mechanism is not taken properly those attacks can still cause great harm in the IoT network. Despite these known attacks, there will be unknown attacks and new security breach which need to be taken into consideration, hence adaptive security measures will be our future to protect IoT network.

References

Abdur Razzaq, M., Habib, S., Ali, M., Ullah, S.: Security issues in the Internet of Things (IoT): a comprehensive study. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **8**(6), 383–388 (2017)

Ahemd, M.M., Shah, M.A., Wahid, A.: IoT security: a layered approach for attacks &amp; defenses. Paper presented at the 2017 International Conference on Communication Technologies (ComTech), 19–21 April 2017

Ahmed, F., Ko, Y.B.: Mitigation of black hole attacks in routing protocol for low power and lossy networks. Secur. Commun. Netw. **9**(18), 5143–5154 (2016)

Ali, B., Awad, A.: Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors **18**(3), 817 (2018)

Arış, A., Oktuğ, S.F., Voigt, T.: Security of Internet of Things for a reliable Internet of Services. In: Ganchev, I., van der Mei, R.D., van den Berg, H. (eds.) Autonomous Control for a Reliable Internet of Services. LNCS, vol. 10768, pp. 337–370. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-90415-3_13

Be-Nazir, N., Ibn Minar, N., Tarique, M.: Bluetooth security threats and solutions: a survey. Int. J. Distrib. Parallel Syst. **3**(1), 127 (2012)

Dowling, S., Schukat, M., Melvin, H.: A ZigBee honeypot to assess IoT cyberattack behaviour. Paper Presented at the 2017 28th Irish Signals and Systems Conference (ISSC), 20–21 June 2017

Dvir, A., Holczer, T., Buttyan, L.: VeRA - version number and rank authentication in RPL. Paper Presented at the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 17–22 October 2011

Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. **80**(5), 973–993 (2014)

Kamble, A., Malemath, V.S., Patil, D.: Security attacks and secure routing protocols in RPL-based Internet of Things: survey. Paper Presented at the 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), 3–5 February 2017

Kammüller, F., Nurse, J.R.C., Probst, C.W.: Attack tree analysis for insider threats on the IoT USING Isabelle. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 234–246. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39381-0_21

Landsmann, M., Wahlisch, M., Schmidt, T.C.: Topology authentication in RPL. Paper Presented at the 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 14–19 April 2013

Li, H., Chen, Y., He, Z.: The Survey of RFID attacks and defenses. Paper Presented at the 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, 21–23 September 2012

Liang, L., Zheng, K., Sheng, Q., Huang, X.: A denial of service attack method for an IoT system. Paper Presented at the 2016 8th International Conference on Information Technology in Medicine and Education (ITME), 23–25 December 2016

Mangelkar, S., Dhage, S.N., Nimkar, A.V.: A comparative study on RPL attacks and security solutions. Paper Presented at the 2017 International Conference on Intelligent Computing and Control (I2C2), 23–24 June 2017

Meidan, Y., et al.: N-BaIoT—network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. **17**(3), 12–22 (2018). https://doi.org/10.1109/MPRV.2018.03367731

Mitrokotsa, A., Rieback, M.R., Tanenbaum, A.S.: Classifying RFID attacks and defenses. Inf. Syst. Front. **12**(5), 491–505 (2010). https://doi.org/10.1007/s10796-009-9210-z

Mustapha, H., Alghamdi, A.M.: DDoS attacks on the Internet of Things and their prevention methods. Paper Presented at the Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan (2018)

Nawir, M., Amir, A., Yaakob, N., Lynn, O.B.: Internet of Things (IoT): taxonomy of security attacks. Paper Presented at the 2016 3rd International Conference on Electronic Design (ICED), 11–12 August 2016

Nurse, J.R.C., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S.: Smart insiders: exploring the threat from insiders using the Internet-of-Things. Paper Presented at the 2015 International Workshop on Secure Internet of Things (SIoT), 21–25 September 2015

Ojo, M., Giordano, S., Procissi, G., Seitanidis, I.: A review of low-end, middle-end and high-end IoT devices. IEEE Access **6**, 70528–70554 (2018)

Olawumi, O., Haataja, K., Asikainen, M., Vidgren, N., Toivanen, P.: Three practical attacks against ZigBee security: attack scenario definitions, practical experiments, countermeasures, and lessons learned. Paper Presented at the 2014 14th International Conference on Hybrid Intelligent Systems, 14–16 December 2014

Raza, S., Wallgren, L., Voigt, T.: SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. **11**(8), 2661–2674 (2013). https://doi.org/10.1016/j.adhoc.2013.04.014

Stubblefield, A., Ioannidis, J., D. Rubin, A.: Using the Fluhrer, Mantin, and Shamir Attack to break WEP (2002)

Thamilarasu, G., Chawla, S.: Towards deep-learning-driven intrusion detection for the Internet of Things. Sensors **19**(9), 1977 (2019). https://doi.org/10.3390/s19091977

Tri-Hai Nguyen, M.Y.: A hybrid prevention method for eavesdropping attack by link spoofing in software-defined Internet of Things controllers. Int. J. Distrib. Sens. Netw. (2017)

Wallgren, L., Raza, S., Voigt, T.: Routing attacks and countermeasures in the RPL-based Internet of Things. Int. J. Distrib. Sens. Netw. **9**(8), 794326 (2013a). https://doi.org/10.1155/2013/794326

Wurzinger, P., Platzer, C., Ludl, C., Kirda, E., Kruegel, C.: SWAP: mitigating XSS attacks using a reverse proxy (2009)

Yair Meidan, M.B., Shabtai, A., Ochoa, M., Tippenhauer, N.O., Guarnizo, J.D., Elovici, Y.: Detection of unauthorized IoT devices using machine learning techniques (2017). https://arxiv.org/abs/1709.04647

Yin, D., Zhang, L., Yang, K.: A DDoS attack detection and mitigation with software-defined Internet of Things framework. IEEE Access **6**, 24694–24705 (2018). https://doi.org/10.1109/ACCESS.2018.2831284

Zhang, K., Liang, X., Lu, R., Shen, X.: Sybil attacks and their defenses in the Internet of Things. IEEE IoT J. **1**(5), 372–383 (2014). https://doi.org/10.1109/JIOT.2014.2344013

Zhou, W., Jia, Y., Peng, A., Zhang, Y., Liu, P.: The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE IoT J. **6**(2), 1606–1616 (2019)

Ray, B., Huda, S., Chowdhury, M.U.: Smart RFID reader protocol for malware detection. In: 2011 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Sydney, NSW, 2011, pp. 64–69 (2011)

Ray, B.R., Chowdhury, M., Abawajy, J.: StenoCipher to provide data confidentiality and tampered data recovery for RFID tag. In: Lee, R. (ed.) Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing 2012. Studies in Computational Intelligence, vol. 443, pp. 37–51. Springer, Berlin (2012). https://doi.org/10.1007/978-3-642-32172-6_4

Ray, B., Chowdhury, M., Abawajy, J.: Hybrid approach to ensure data confidentiality and tampered data recovery for RFID tag. Int. J. Netw. Distrib. Comput. **1**(2), 79–88 (2013)