Journal of Robotics and Control (JRC)
Volume 2, Issue 1, January 2021
ISSN: 2715-5072 DOI: 10.18196/jrc.2150

Survey on IoT: Security Threats and Applications

Irfan Ahmad[1]*, Mohammad Saber Niazy[2], Riaz Ahmad Ziar[3], Sabawoon Khan[4]
[1, 2, 4] Department of Computer Science, Khurasan University, Nangarhar, Afghanistan
[3]Faculty of Engineering and Technology, Kardan University, Kabul, Afghanistan
Email: [1]irfan.ahmed.mcse@gmail.com, [2]niazi.edu@gmail.com, [3]r.ziar@kardan.edu.af,
[4]sabawoon.pasoon@gmail.com
*Corresponding Author

***Abstract*— the rapid growth of the internet of things (IoT) in the world in recent years is due to its wide range of usability, adaptability, and smartness. Most of the IoT applications are performing jobs an automatic manner without interactions of human or physical objects. It's required that the current and upcoming devices will be smart, efficient and able to provide the services to the users to implement such a new technology with a secure manner. Thus the security issues are exploring day by day by the researchers. IoT devices are most portable and light in nature so it has several issues such as battery consumption, memory, and as these devices are working open range so the most important is security. In this survey paper, we have elaborated on the security attacks with reference to the different kinds of IoT layers. In the last, we have presented some of the applications of the IoT. This study will provide assistance to the researchers and manufacturers to evaluate and decrease the attacks range on IoT devices.**

Keywords*— *IoT, smart Homes, healthcare, Encryption, Security

I. INTRODUCTION

Internet of things (IoT) is a new trend nowadays in the word. As the technology is spreading everywhere and it's become a crucial requirement to connect with the internet for societies, health care, universities, houses even for each and everything. According to the [1] report, the expected things that will be connected are 8.4 billion all over the world in 2020 and this number will be approximately increased to 20.4 billion in 2022. Increment in the usage of IoT applications in all the scenarios over the worldwide, the growth of connectivity between the machines is expected from 5.6 billion and will be increased up to 27 billion from 2016 to 2024 [1]. The wide range of IoT Application usage some privacy & security, authentication, and storage issues have been raised and it's a challenging topic, for now, a day between the research communities. Without a secure environment and infrastructure, it's very difficult to use the IoT application with full features and in a trustable manner. According to [2] in 2017 attacks against IoT devices has been increased by 600 percent. Usually, attackers are not targeting IoT edges directly but use it as a weapon to access other sites. IoT devices will be easily targeting due to their manufacturer's nature because most of the companies are not considering security and forensics for devices while most of them are giving stress to cost, size, and usability. If we look into behind our daily life we will see a lot of IoT devices attached to our daily life such smart electricity meters which use to control power utilization, lighting, and other resources. Security cameras are another IoT device that will notify you of unwanted movement at night, smart fridges also giving notification when you face with a shortage of drinking & milk, sensor doors that opens with your sound and face recognitions. Guess it, if a company compromises on its security and makes it based on price and size so, in the IoT era, it will affect all the physical objects in which you are dealing with your daily life. Modern cars are also using the sensors if the car sensors and programs hacked by someone so, in fact, your life is at risk. Improving nowadays in healthcare some of the sensors are used for providing the report to doctors if it is targeted so the patient life is at risk. Not only in the healthcare unit the IoT security is more crucial in business life attackers may steal your bank details and perform un-authenticable transactions. In fact, these types of cyberattacks are most dangerous to large companies as one case from US history, which performs in 2013; a group of attackers has stolen $160 million from credit card [2]. The main contribution of the paper is that we have elaborated the different security issues related to the IoT layers infrastructures and some of the application of the IoT era.

Simply in today's technological era each and everything is under a cyberattack and can be a threat.

II. IOT SECURITY

Due to billions of IoT smart devices communications the security of IoT is the most essential and challenging task for the research community. As IoT is in fast-growing stage and demand of smart devices also increasing so the manufactures oversight the security aspects and delivering the vulnerable devices in the market attackers easily targeting the devices using these vulnerabilities and performing a large number of DDoS and other types of Attacks to steal user personal information and data from IoT

devices. Figure 1 shows the classification of different types of IoT attacks with aspects of layer architecture.

A. **Physical Attacks**: Physical attacks are a type of attack in which the attackers robust on the system hardware instead of software.

- **Node Tampering:** In this type of attack the attackers damaging the sensor nodes, it will be physically damaged or electronically grill the nodes to take the access and modify the important information e.g. confess the shared crypto keys this might damage the whole sensors [3].

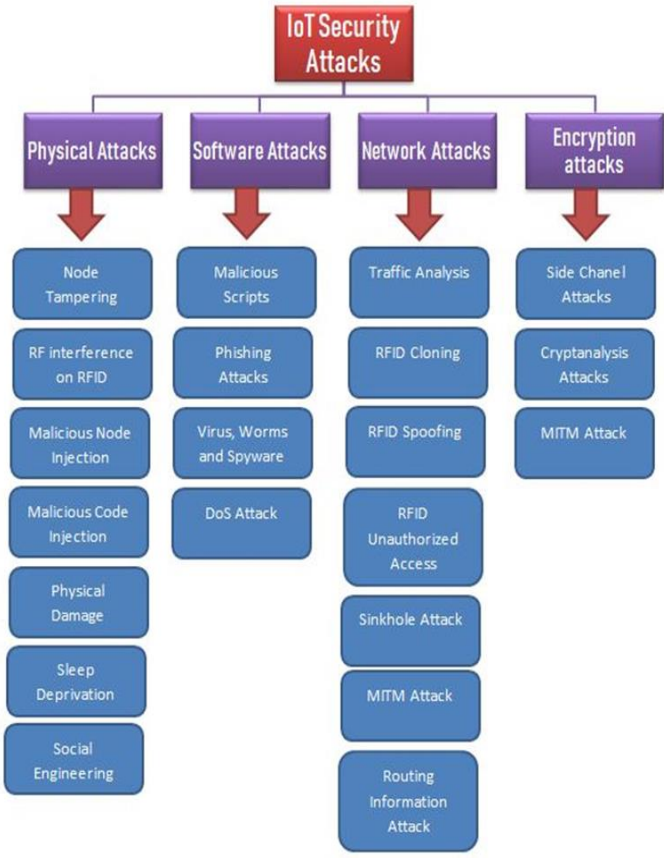

Figure 1. Classification of different type of IoT attacks with aspects to layer architecture.

- **Malicious Node Injection:** In this type of Attack the attackers installing the malicious node between two or more nodes and monitoring the traffic to and from the nodes. This type of attacks also known as Man in the Middle-Attack [3].

- **Malicious Code Injection:** In this type of attack the attackers trying to inject malicious code in the node memory. As the IoT devices software's are updating in an open area so this will provide the whole to attackers to inject the malicious code and with this attacker trying to gain the overall IoT system control [1].

- **Sleep Deprivation:** In IoT, most of the devices are using the battery for power purposes, for the best life the devices need to follow the sleep cycle. In sleep deprivation attack the attacker keeps the devices active; this will cause the more usage of battery life and in the result, devices go to shut down [4].

- **Physical Damage:** As from the name in this type of attack the attackers are trying to gain data by some physical actions. Attackers starting from organization waste bins for searching to find out some information such as date of birth, security numbers for validating the computer passwords [5].

- **Social Engineering:** In these attacks the attackers targeting people instead of a computer system for getting the information. Attackers are trying to shape the target into the fake network and perform some malicious activities for gaining the data [5].

B. **Software Attacks**: In these types of attacks, the attackers are trying to steal data or deny the service by using some viruses, spyware, and other malicious codes.

- **Virus, warms & Spywares:** Attackers are trying to send some malicious files as an email attachment when the recipient receives the email and download the attachment or download other files from the internet so it will affect the system. Different methods can be used to detect these types of attacks like firewall, antivirus and other detection system proposed by researchers [6].

- **Malicious scripts:** In this type of attack the adversary using malicious scripts with the normal query. When normal quires are executing so the scripts run automatically like normal quires and making a threat to the users. According to the Imperva Web Application Attack Report (WAAR) round, about 96.15 % Web attacks have been performed [7].

- **Phishing attack:** This type of attack usually uses to strip the user's important information such as Credit card details, email passwords, etc. in this type of attack the emails or website is used. Adversary makes the phishing sites exactly like the original one and track the users. The adversary can use the emails, website and also phone calls [8].

- **DoS Attack:** In denial of service attack, the adversary sending unusual traffic on systems, which makes the resources unavailable to other users. In denial of service attack, the adversary can also mislead the data and tempering it for resending [9].

C. **Network Attacks:** IoT devices are moving in various places and connected through the internet so it more vulnerable to attacks. Some of the network attacks are discussed below

- **Traffic Analysis:** In this type of attack, the adversary is trying to get the packet pattern and change the contents. As some of the packets are encrypted but we cannot say that is secure from attacks [10].

- **RFID Cloning:** This type of attack is using the tags to portray certain tags can edge to threats that are not manageable.

- **RFID Spoofing:** In this type of attack, RFID tags are not physically replicated. In spoofing attack the adversary using the special devices with more features that are capable to mirror the RFID tags to gain some data. The adversary is trying to get the original RFID tag access and thorough that will take privileges. With the help of this technique, the adversary is taking full access on data channels as the original tag [11].

- **RFID Unauthorized Access:** as RFID tags are responsible to send and receive data with different signals so there are more chances of someone places the RFID card reader and steals the data.

- **Sinkhole Attack:** This attack occurs on the RPL routing protocol in IoT, the adversary is trying to install a malicious node in between the real nodes to broadcast the fake routes. As a result, most of the hops are sending & receiving the traffic through the attacker node. IoT devices Performance also will be affected in this type of attack [12].

- **MITM Attack:** In this type of attack, the adversary is sitting between the nodes and interpreting the communication between the two parties. When the sender is sending information the adversary is receiving it and after modification transfers it to the receiver rather than the actual value. When the receiver is replying so the adversary is doing the same process and replies to the sender. Most of the time this type of attack performs for stealing the login details of credit cards or other personal information [13].

- **Routing Information Attack:** In this type of attack, the adversary is trying to change the traffic directly into a fake route and gain access to the secret data [14].

D. Encryption Attacks: Actually, in this type of attack, the adversary is trying to gain access to the plain text which will be from several ways like stealing the key, finding the weakness in the code, cryptographic protocols issues, etc.

- **Side channels attack:** In this type of attack the adversary targeting the physical security implementation to leak the personal and sensitive information. This attack has become more attractive in recent years [15].

- **Cryptanalysis** attack**:** In this type of attack the attackers are trying to find out the weakness in crypto algorithms and deduce the crypto keys [16].

- **MITM Attack:** Man in the Middle attack the adversary is trying to hijack the public value. Instead of the original public value, the attackers developing their own keys and sending it to the receiver and vice versa in reply states [17].

III. APPLICATION AREAS OF IoT

Security and privacy are the crucial requirements for all IoT devices and applications which are in use or will be used soon. With the rapid change in the technology word the usage of IoT applications is also increasing day by day. All manufacturers are trying to improve the security level of the devices, but some of the applications are very sensitive and especially in the health care system thus need high-security requirements. Some of the IoT applications are discussed as follow.

- **Smart Homes:** Nowadays the most usable and efficient application of IoT is smart homes. According to the [18] report, people searched the smart home 60,000 times and one more interesting point is round around 256 companies are working in smart home appliances and startups. Companies are investing round about $2.5 billion in the growth of IoT rate. Most of the electronics companies e.g. Haier, Samsung, Philips, etc. are now bulleting the features for IoT Uses, it helps IoT in rapid growth.

- **Smart City:** Smart cities are another application of IoT which are in rapid growth in the world. As from the name, is a smart city are using wireless sensors device to connect all the components of the city. According to the [19] report from the International Data Corporation (IDC) roundabout, 180+ smart cities are designed and more than $135 billion will be expected to be spent until 2021. Basically, smart cities are improving the citizen and visitors' life, each and everything will be smart from one another.

- **Smart Grids:** Smart grids are another application of IoT. Smart grids are functioning automatically and help in electricity distribution, efficiency, and control the wasting of electricity in a more reliable way. According to the [18] round, about 41000 people have searched the concept of the smart grid on google in one month which shows the growth of the application. Security to this era also a very important step because if the controlling of the system goes to the adversary's hands maybe it will create big damage.

- **Health Sector:** one of the most and reasonable applications of IoT in the health system. As the world is moving to the technology phase bay by day, most of the changes have been recorded in the health system. It’s very important to increase the security level of these applications as we look into the system, wireless sensors

are placing in the patient's body and connecting into the cloud for transferring the patient information to the doctor. If the accurate information is not transferred to the doctor so how he will recommend the valid medicine. If we look into another side if valid information has received to the doctor and he referred the medicine and it was hacked in the way and the adversary will modify the medicine report so it is also a high risk for the patient.

- **Security & Emergencies:** Security & emergencies are another application in the IoT system. Today's most of the army operations are especially in the demining filed used most of the machines for such a task, or also are installing the wireless sensors to prevent unauthorized access to the prohibited areas. In most of the buildings, wireless sensors are installed to handle the thief activities, control lighting system, water system, and much more.

IV. IOT SECURITY

As we have elaborated on some of the security issues in the previous section, in this section, we are going to present some of the ways for securing IoT applications and the environment. There are four main techniques for protecting the IoT environment 1) Edge computing, 2) Fog computing, 3) Blockchain & 4) Machine learning. Below are some detailed discussions on stated techniques.

A. IoT Security Using Fog Computer

In the internet of things, most of the users and devices are portable and also data stored in cloud computing. Thus there is more issue to be addressed such as security, power consumption, bandwidth, and reliability. In [20], the authors proposed the three layers of architecture which will be work between the sender and receiver to overcome the storage, computation burden, limited resources, and security & privacy issues. In [21] introduces a method by name COLOR +, which is used to perform most of the computation on the terminal node. COLOR + is also used to detect the spammers on suspension based. According to their results, COLOR + accuracy are 85.95 % in detection methods. In [22] the author proposed the CP-ABE key exchange protocol for authentic communication between the users. They also combined digital signature and CP-ABE methods to achieve confidentiality and verifiability. In [23] they have proposed the novel architecture for securing the fog computing communication and data sharing.

B. IoT Security Using Machine Learning

As we have elaborated above that Dos attack is one of the most used methods of stolen the data in the IoT environment. For securing such serious attack the Multi-Layer Perceptron (MLP) is used [24]. The authors of [24] proposed the particle swarm optimization and backpropagation algorithm that increase wireless network security. Another type of attack that established in IoT is Eavesdropping. The adversary may drop the packets during the communication. To be safe from this type of attack ML techniques such as Q-learning based offloading strategy [25] or non-parametric Bayesian techniques [26] can be used.

C. IoT Security Using Edge Computing

As in edge computing, the data transmission is with in-network or in the device. The movement of data is less as compared to the fog computing and this will reduce the security issues [27]. Another issue is data compliance in some countries that they don't want to share the data with other countries and have some restrictions on it. So using edge computing the data compliance issue will be solved [28]. Another issue that is solved with edge computing safely issues [29]. If the user does not have the fast internet connection and each and everything will transfer to the cloud and will wait for the response so may it will affect the safety of a person or group.

D. IoT Security Using Block chain techniques

Blockchain technology is the most important improvement in the IoT security era. Which focuses all on IoT implementation in a secure way? In simple term Blockchain in a dairy of transactions which keeps all transaction as a hash. In [30] the author introduces a new system for access management that moderates the various issues related to the IoT devices. The solution of the paper is decentralized and based on Blockchain technology. As one of the big issues in the IoT ecosystem is a single point system the [31] author has introduced a new decentralized system for IoT by name of privacy-preserving publish/subscribe using Blockchain technology.

V. CONCLUSION

In this survey paper, we have elaborated on the security threats to the IoT devices concerning different IoT layers e.g. physical, software, network & encryption layers. We have also discussed some of the applications of IoT. We are expecting this survey will be helpful for IoT researchers & Manufacturers for enhancing the security level in future IoT appliances.

REFERENCES

[1] V.HASSIJA1, V.CHAMOLA, V.SAXENA, D.JAIN, P.GOYAL & B.SIKDAR, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE*, vol. 7, pp. 82721 - 82743, 2019.

[2] M.Stoyanova, Y.Nikoloudakis, S. Panagiotakis, E.Pallis, & E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues," *IEEE*, pp. 1-38, 2020.

[3] D.Sopori, T.Pawar, M.Patil, & R.Ravindran "Internet of Things: Security Threats," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 6, no. 3, pp. 263-267, 2017.

[4] A.Jain, B.Sharma, & P.Gupta "INTERNET OF THINGS: ARCHITECTURE, SECURITY GOALS, AND CHALLENGES- A SURVEY," *International journal of innovative research in Sciense and Engineering* , vol. 2, no. 4, pp. 154-163, 2016.

[5] K.Krombholz, H.Hobel, M.Huber, & E. Weipp "Social engineering attacks on the knowledge worker," in *Proceedings of the 6th International Conference on Security of Information and Networks*, Aksaray, Turkey, 2013.

[6] J.Deogirikar, & A.Vidhate "Security Attacks inIoT: A Survey," in *International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, India, 2017.

[7] B.Yong, X.Liu, Q.Yu, L.Huang, & Q.Zhou "Malicious Web traffic

detection for Internet of Things environments," *Computers and Electrical Engineering*, vol. 77, p. 260–272, 2019.

[8] T.Nathezhtha, D.Sangeetha, V. Vaidehi "WC-PAD: Web Crawling based Phishing Attack Detection," in *International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India, 2019.

[9] S.A.Butt, & A.Ali, "IoT Smart Health Security Threats," in *International Conference on Computational Science and Its Applications (ICCSA)*, Saint Petersburg, Russia, Russia, 2019.

[10] F.Kausar, S.Alzaydi, S.Aljumah, & R.Alroba "Traffic Analysis Attack for Identifying Users' Online Activities," *IEEE IT Professional* , vol. 21, no. 2, pp. 50-57, 2019.

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

[12] S.R.Taghanaki, K.Jamshidi, & A.Bohlooli "DEEM: A Decentralized and Energy Efficient Method for detecting sinkhole attacks on the internet of things," in *IEEE*, Mashhad, Iran, Iran, 2019.

[13] N.Naher, Asaduzzaman, M.M Haque. "Authentication of Diffie-Hellman Protocol Against Man-in-the-Middle Attack Using Cryptographically Secure CRC. In: Chakraborty M., Chakrabarti S., Balas V., Mandal J. (eds) Proceedings of International Ethical Hacking Conference Advances in Intelligent Systems and Computing, vol 811. Springer, Singapore 2018.

[14] C.Pu, "Spam DIS Attack Against Routing Protocol in the Internet of Things," in *International Conference on Computing, Networking and Communications (ICNC)*, Honolulu, HI, USA, USA, 2019.

[15] Lo'ai A. Tawalbeh, T.F. Somani, "More secure Internet of Things using robust encryption algorithms against side channel attacks," in *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, 2016.

[16] A. Fox, "efficientgov," 21 May 2018. [Online]. Available: https://www.efficientgov.com/emergency-management/articles/cryptanalysis-attacks-protecting-government-data-encryption-gIzjjTqR78a0H0Cs/. [Accessed 5 May 2020].

[17] N.NaherEmail, Md.Asaduzzaman, & Mokammel Haque "Authentication of Diffie-Hellman Protocol Against Man-in-the-Middle Attack Using Cryptographically Secure CRC," in *Proceedings of International Ethical Hacking Conference*, Springer, Singapore, 2018.

[18] R. Gour, "dzone," 30 Oct 2018. [Online]. Available: https://dzone.com/articles/top-10-uses-of-the-internet-of-things. [Accessed 5 May 2020].

[19] T. Maddox, "techrepublic," 16 July 2018. [Online]. Available: https://www.techrepublic.com/article/smart-cities-the-smart-persons-guide/. [Accessed 5 May 2020].

[20] G.Zhuo, Q.Jia, L.Guo, M.Li†, & Pan Li "Privacy-preserving Verifiable Data Aggregation and Analysis for Cloud-assisted Mobile Crowdsourcing," in *The 35th Annual IEEE International Conference on Computer Communications*, San Francisco, CA, USA, 2016.

[21] Zhang, J., Li, Q., Wang, X. et al. Towards fast and lightweight spam account detection in mobile social networks through fog computing. Peer-to-Peer Netw. Appl. 11, 778–792 (2018). https://doi.org/10.1007/s12083-017-0559-3

[22] A.Alrawais, A.Alhothaily, C.Hu, X.Xingx, and X.Cheng, "An Attribute-Based Encryption Scheme to Secure Fog Communications," *IEEE Access*, vol. 5, pp. 9131 - 9138, May, 2017.

[23] A.Alotaibi, A.Barnawi, M.Buhari, "Attribute-Based Secure Data Sharing with Efficient Revocation in Fog Computing," *Journal of Information Security*, vol. 8, pp. 203-222, 2017.

[24] R.V. Kulkarni, G.K.Venayagamoorthy, "Neural Network Based Secure Media Access Control Protocol for Wireless Sensor Networks," in *Proceedings of International Joint Conference on Neural Networks*, Atlanta, Georgia, USA, June 14-19, 2009.

[25] L.Xiao, C.Xie, T.Chen, H.Dai H. V.Poor, "A Mobile Offloading Game Against Smart Attacks," *IEEE Access*, vol. 4, pp. 2281 - 2291, 09 May 2016.

[26] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, `Proximity-based security techniques for mobile users in wireless networks," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 2089-2100, Dec. 2013.

[27] G.Premsankar, M. Di Francesco, and T.Taleb, "Edge Computing for the Internet of Things: A Case Study," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1275 - 1284, April, 2018.

[28] L. Rosencrance, " 6 significant issues that edge computing in IoT solves, 01 Nov 2018. [Online]. Available: https://internetofthingsagenda.techtarget.com/feature/6-significant-issues-that-edge-computing-in-IoT-solves?_ga=2.53786920.1250231981.1589957400-683346247.1588924221. [Accessed 20 May 2020].

[29] N.Abbas, Y.Zhang, A.Taherkordi, and T.Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450 - 465, 2018.

[30] O. Novo, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," *JOURNAL OF INTERNET OF THINGS CLASS FILES*, vol. 14, no. 8, pp. 1-12, MARCH 2018.

[31] P.LV, L.WANG, H.ZHU, W.DENG, and L.Gu, "An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Blockchains," *IEEE Access* , vol. 7, pp. 41309 - 41314, March 2019.