International Engineering Journal For Research & Development
Vol.4
Issue 2

E-ISSN NO:-2349-0721

Impact factor : 6.549

SECURITY ISSUES IN USING IOT ENABLED DEVICES AND THEIR IMPACT

Vishal Dineshkumar Soni
Department of Information Technology, Campbellsville University, Campbellsville, Kentucky

---

ABSTRACT

With rapid growth of science and information technology, Internet of things (IoT) becomes as an integral part of daily life. The applications of IoT are expanded starting from connected cars, wearables, connected health, smart retail and healthcare. However, security issues are increasing with the increase of its use. Lack of compliances on the part of IoT manufacturers, lack of user knowledge and awareness, device update and management, lack of physical hardening and botnet attacks are considered as the major reasons for security issues in IoT based applications. In this aspect, it becomes important to analyze security issues involved with IoT and its impact on the users that has been performed in the present study.

Keyword: Internet of things, RFID, security issues, heterogeneous features, cryptography

INTRODUCTION

In 1999, Kevin Ashton firstly introduced the idea of the Internet of Things. The use of IoT is increased with the advancement of Wireless Sensor Networks, Radio Frequency Identification (RFID), cloud computing, and mobile communication as well as IoT devices can cooperate with other devices. To communicate with each other IoT depends on wireless communication systems and cost-effective sensors. A huge variety of devices is present in IoT such as personal computers, laptops, PDAs, smartphones, tablets, and other hand-held embedded services. A major part of applications and devices are not designed properly to maintain security and privacy factor, which is able to increase security and privacy issues in IoT such as authentication, access control, data integrity, secrecy, confidentiality, etc. this paper has been described several security issues, challenges, and considerations. Various characters of IoT are included in this paper as well as this paper also contains all kinds of security attacks.

BACKGROUND OF IOT

The global infrastructure of interconnected networks of virtual and physical objects is identified by the internet of things. These objects are connected with the help of wired or any wireless network system to transfer information among various IoT devices, which help to produce novel services and applications. Along with these digital machines, computing devices and other objects are interrelated by the Internet of Things. The Internet of Things is involved in generating, exchanging, and consuming data with low human interventions. IoT consists of a huge amount of opportunity as well as a broad scope of issues and challenges are also present in IoT. Five emerging issues of IoT are most important among all issues such as interoperability, emerging economics, privacy, security, and legal and regulatory rights. A large amount of user data is accessed with the help of the Internet of Things. Interoperability is considered a major concern during the implementation of IoT. Sometimes, IoT leaves a negative impact due to poor design, network resources, and internet resources. Various legal and regulatory questions are increased due to the implementation of IoT, such as civil rights and law

enforcing surveillance conflicts, cross border data flows, retention of data, data misuse, legal liabilities and unintended uses, laps of privacy, and architecture related issues.

3. Essential characters of IoT

IoT is used to enhance people's quality of life; new applications are generated by IoT that can control the all-important activity of people. This Internet of Things is consisting of a few common characteristics, which are described below:

(i) **Large scale:** Now, use of IoT devices is increasing rapidly. It is important to control these large-scale devices, which help devices to communicate with each other. Along with this, a huge amount of data is generated by this large scale network. Critical issues related to data interpretation and analyses are produced by this generated data.

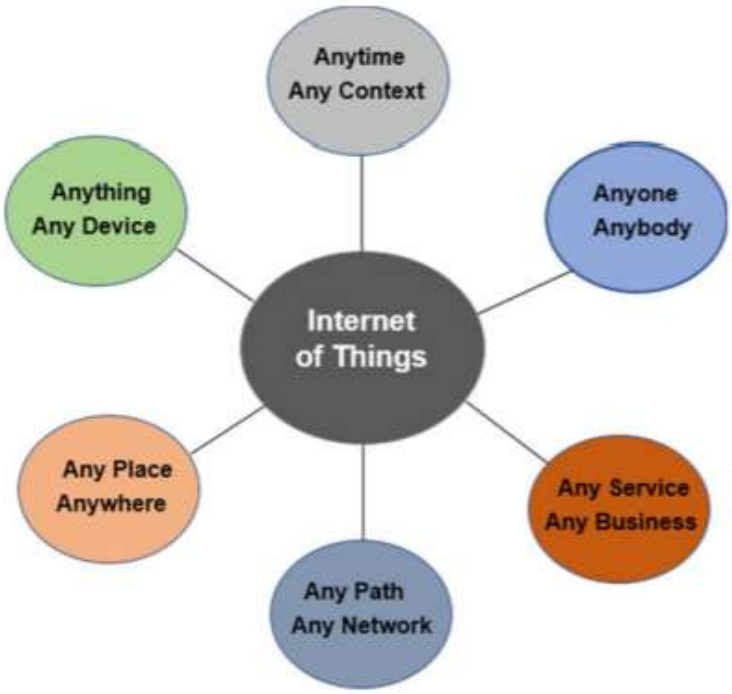

Figure 1: Use of internet of things

(Source:Frustaci et al. 2017, p.330)

(ii) Intelligence: IoT devices are enhancing their performance with the help of sophisticated software algorithms and high-performing hardware. This enhancement helps IoT to make intelligent decisions in important situations. In addition, IoT can communicate with other devices through this enhancement process.

(iii) Complex system: Huge numbers of heterogeneous objects with various software and hardware capabilities are involved in the IoT system.

(iv) Dynamic environment: Almost all objects of our environment are connected with IoT, without determining the network boundaries of IoT that can make this technology dynamic in nature. Based on changing conditions and environments, the IoT system is operated dynamically.

(v) Sensing: IoT can maintain changes in surrounding environments and produces data with the help of sensors, which is a major part of IoT. A good understanding of the surrounding environment is provided by sensors by using high-performing sensor technologies. This factor can enhance human awareness about the physical world.

(vi) Heterogeneity: A huge number of devices with heterogeneous features are involved in IoT, these heterogeneous features are communication protocol, operating system, platform, and others. Management operates complex tasks to perform with the presence of heterogeneous features.

(vii) Unique identity: unique identities such as IP addresses are used in the IoT network to identify and recognize all objects of the IoT system. IoT manufacturers are involved in providing these identities that can take place in upgrading devices in an appropriate platform. Important and required information is collected by users from the device with the help of proper interfaces of the device. This information help users record their status and manage this recorded information remotely.

SECURITY ISSUES, CHALLENGES, AND CONSIDERATIONS

The rapid growth of internet-connected devices is involved in the enhancement of IoT. In addition, security issues are considered the most important factor in IoT; these issues are now increased due to presence of different stakeholders in the Internet of Things that can slow down the adoption of IoT. Frustaci et al. (2017) stated that fundamental factors of an IoT system are its security aspects, which are treated as basic requirements to enhance trust and privacy quality of a system. IoT security needs to secure the data protection, connected devices, and network of IoT.

Products that are designed and developed by such teams quickly lose the customer's trust. One of such example is the Bluetooth-enabled door locks. The company faced strong criticism about the product that it was highly insecure and hacking it was possible easily. It was one of the most damaging claims made regarding the product, which was designed only to establish security. The failure of the Bluetooth-enabled door lock system was not because of the actual technology, but because of its poor implementation by the manufacturers. Such kind of damage to the name of the manufacturers can also severely affect all the other devices the company produces other than the ones that work over the network.

In information technology, the context of security has always been a matter of concern. This concern has not pardoned even the concept of IoT. The implementation of IoT concepts has introduced new and unique security challenges, addressing which is the fundamental priority. Devices with inadequate security could open a gateway for malicious users to abuse the enormous amount of data. The safety of issue arises with the interconnected nature of IoT. Moreover, the homogeneity of devices, the ability to auto connects and fielding devices in unsecured networks make the security concern more challenging. Hence, it is a collective obligation of developers and users to take care of the fact that devices stay away from potential harm leading to a collaborative approach to security.

It is important to maintain poor security behavior in both the whole system and individual behaviors. Huge numbers of devices are connected with IoT in new locations and applications, which ensure that the complexity of the system is increased day-by-day. Due to the design system of IoT, traditional security mechanisms cannot be implemented in IoT technologies. Besides, a huge number of connected devices and limited power can increase heterogeneity and scalability issues in systems. A wide range of risk is increased in this case that can

decrease the security and safety of the system. System elasticity is treated as a strong consideration (Khan and Salah 2018).

Heterogeneity is an important and critical issue that can leave an impact on mechanisms, which is integrated into IoT. Network security services that have to be used in Internet of Things are affected by heterogeneity. Interaction between heterogeneity devices and constrained devices is conducted through gateways or directly. Heterogeneity is unable to implement effective algorithms and protocols in all fields of IoT application, to overcome this problem high-performing security are needed for heterogeneity. Implementation of high-quality cryptographic algorithms can adapt lightweight security protocols and high throughput. End-to-end secure communication is provided by this security factor.

The main problematic issue of IoT is security threats as this system is using a minimum capacity of devices. Openness of the system and physical accessibility to sensors is considered that the device will communicate wirelessly. Deployment of IoT security is hindered by various security concerns such as man-in-the-middle attack, DoS/DDoS attack, heterogeneous network issue, WLAN application conflicts, and application risk of IPv6. Besides platform management, information and user authentication are also considered as an application security issue of IoT (Zhou et al. 2018).

Data security issues are classified into four groups such as data availability, integrity, authenticity, and confidentiality. The employment of security measures can solve this security issue. Data confidentiality can protect data from unauthorized users; on the other hand, correctness and accuracy of data are maintained by the data integrity process. Information about the restraint of authorized access to network resources, applications, and services are guaranteed by data availability (Qian et al. 2018). Along with this, authenticity ensures that only authorized entities are able to access network resources. Therefore vulnerable data theft leaves an impact on a large number of IoT applications and services. Advance technology is required in a few fields to mitigate this kind of attack that can provide ultimate security towards the Internet of Things. Identification, availability, confidentiality and integrity are involved in the security of information and network. IoT security consists of a few important problems such as confidentiality, authentication, and data integrity (Bakhshi et al. 2018). Connection between devices and exchange number of publics is maintained by authentication, authentication can maintain private keys with the help of nodes to mitigate data steal. Confidentiality is able to provide information about unauthorized objects which conceal IoT devices. Safeguarding of data is maintained by data integrity.

IOT SECURITY ATTACKS AND THEIR IMPACT

Weak communication channels are created in the IoT system due to distributed and dynamic nature, this communication is used by malicious objects to increase new threats regarding tracking, reporting, and monitoring of the user's actions (Kumar and Mallick 2018). A set of security attacks is occurred due to the increasing use of the Internet of Things in communities that need to be considered. Security attacks of IoT are classified into four groups such as software attack, physical attack, encryption attack, and network attack. These security attacks are described below and the summarization of all security attacks in the IoT system is provided in figure 2.

Physical attacks: this type of attack is mainly .increased by hardware elements of Internet of Things; in this case, to conduct the attack physical appearance of the attacker is required. Expensive substances are required in

this attack, which increases the difficulties of this attack. Physical attack consists of a few important factors which describe below:

- Node tempering: sponsor nodes are targeted by attackers to damage it or replace the entire node.
- Malicious node injection: A new operating node is operating physically among communication nodes of IoT which help attackers to enhance the access to sensitive information. Data flow between several nodes is controlled by attackers.
- Physical damage: This process is difficult to achieve all requirements of attackers to reach an area (Vashi et al. 2017). In this attack, attackers are trying to harm this attack directly which leaves an impact on system availability and quality of services which is a main difference between this attack and node tempering attack. Despite these physical attacks consist of RF interference on RFID, malicious code injection, sleep deprivation, and social engineering.

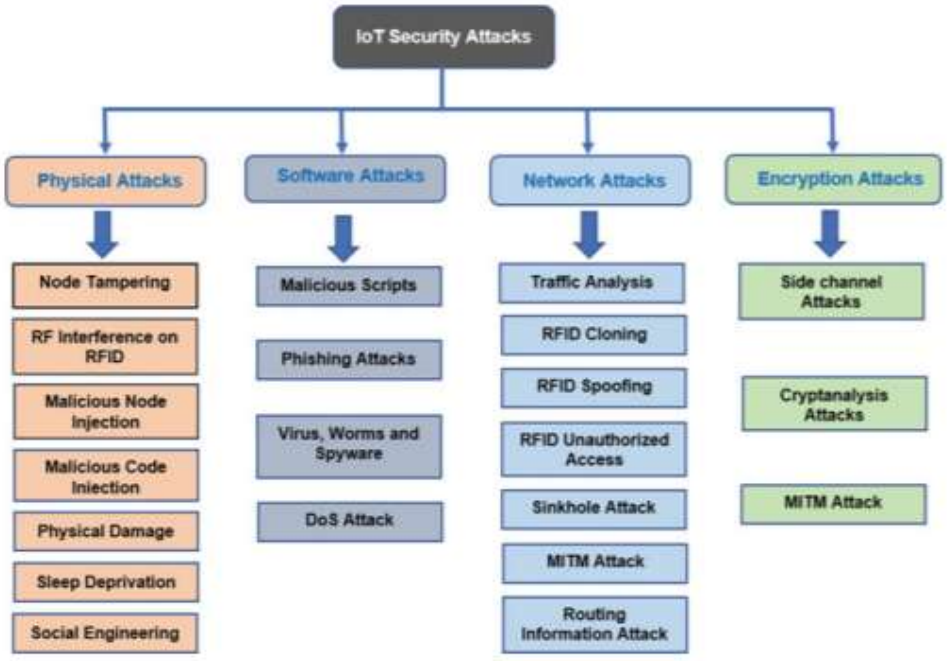

Figure 2: Security attacks in IoT

(Source: Ge et al. 2017, p. 456)

SOFTWARE ATTACKS

Security threats are mainly conducted by software attacks. Weakness of the system is targeted by this attack with the help of communication interfaces. Software attack consists of four types such as malicious scripts, phishing attacks. According to Ge et al. (2017), viruses, spyware and worms, and DoS attack. Malicious script is used by attackers to access sensitive data and disturb system availability. Virus, spyware, and worms attack is related to a malicious code injection attack. In this attack to gain accessibility, attackers inject the system with malicious software (Oh and Kim 2017).

NETWORK ATTACK AND ENCRYPTION ATTACK

The IoT system is a combination of networks, which can maintain data transfer between various IoT devices. This attack is conducted with seven elements such as traffic analysis attack, RFID Spoofing, RFID unauthorized access, RFID cloning, MITM attack, Routing Information Attacks, and a Sinkhole attack. On the other hand, with the help of communication channels, the IoT system is connected with all objects (Frustaci et a. 2017). In this case, encryption algorithms are used to protect this communication. Encryption attack is trying to reach the encryption structure, which is used in IoT systems. This attack consists of three factors such as side-channel attacks, MITM attack, and cryptanalysis attack.

IMPACT OF SECURITY ISSUES OF IOT ON USERS

This security issue of IoT directly has an impact on the confidence of industries. According to the latest research report, 54 percent of consumers provide negative reports about IoT implementation. 65 % of consumers stated that hackers monitor their IoT devices. 60 % of consumers' data is leaked. Risk of the cloud attack is increased, due to this poor security of IoT, which increased costs related to cybercrime (Khan et al. 2018). Risk of losing important data is increased due to poor design and security of the Internet of Things.

CONCLUSION

Use of IoT is increased due to the advancement of wireless sensor networks, radio Frequency Identification, cloud computing, communication, and mobile communication. These factors help IoT to communicate with other devices. Based on this paper it is concluded that IoT devices and applications are nor designed properly to handle security and privacy-related issues in IoT networks. Various security attacks can leave an impact on this IoT system, these security attacks are physical, network attacks, encryption attacks, and software attacks, which is concluded in this paper. Several security issues, challenges, and considerations are also concluded in this paper.

REFERENCES

1. Bakhshi, Z., Balador, A. and Mustafa, J., 2018, April. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (pp. 173-178). IEEE.
2. Frustaci, M., Pace, P., Aloi, G. and Fortino, G., 2017. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of things journal, 5(4), pp.2483-2495.
3. Frustaci, M., Pace, P., Aloi, G. and Fortino, G., 2017. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of things journal, 5(4), pp.2483-2495.
4. Ge, M., Hong, J.B., Guttmann, W. and Kim, D.S., 2017. A framework for automating security analysis of the internet of things. Journal of Network and Computer Applications, 83, pp.12-27.
5. Khan, M.A. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, pp.395-411.
6. Khan, M.A. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, pp.395-411.
7. Kumar, N.M. and Mallick, P.K., 2018. Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, pp.1815-1823.

8. Lamba, A., Singh, S., Balvinder, S., Dutta, N. and Rela, S., 2018. Embedding Machine & Deep Learning for Mitigating Security & Privacy Issues in IoT Enabled Devices & Networks. International Journal For Technological Research In Engineering.
9. Oh, S.R. and Kim, Y.G., 2017, February. Security requirements analysis for the IoT. In 2017 International Conference on Platform Technology and Service (PlatCon) (pp. 1-6). IEEE.
10. Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M. and Pustišek, M., 2018. Towards decentralized IoT security enhancement: A blockchain approach. Computers & Electrical Engineering, 72, pp.266-273.
11. Vashi, S., Ram, J., Modi, J., Verma, S. and Prakash, C., 2017, February. Internet of Things (IoT): A vision, architectural elements, and security issues. In 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 492-496). IEEE.
12. Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2018. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2), pp.1606-1616.