Internet of Things: Security Threats

Diksha Sopori, Tanaya Pawar, Manjiri Patil, Roopkala Ravindran

Abstract—This paper aims to address the need for tightening the Security and Privacy issues of IoT applications. During the past decade, IoT has been developed rapidly but it did not consider the profound security goals and challenges involved appropriately. Security and privacy are the key issues for IoT applications, and still face some enormous challenges. In order to this emerging domain, this study explores the security aims and goals of IoT, the current security status and the attacks that makes the IoT applications vulnerable.

Keywords- ***Encryption, Industry 4.0, Internet of Things, Security***

I. Introduction

The term, internet of things (IoT) that refers to uniquely identifiable objects, things, and their virtual representations in an internet-like structure, was first proposed in 1998. Internet of Things allows electronic devices to exchange information in the surrounding environment with other members of the network making it possible to recognize events and changes in their surroundings and to act and react autonomously without requiring human-to-human or human-to-computer interaction. The Internet of Things enabled by Wireless Sensor Networks (WSN) and RFID sensors finds a plethora of applications in almost all the fields such as health, education, transportation and agriculture. The advantages of IoT are innumerable and its applications are changing the way we live and work by saving time ,cost and resources, and opening new opportunities for growth, innovation, and the exchange of knowledge between entities.

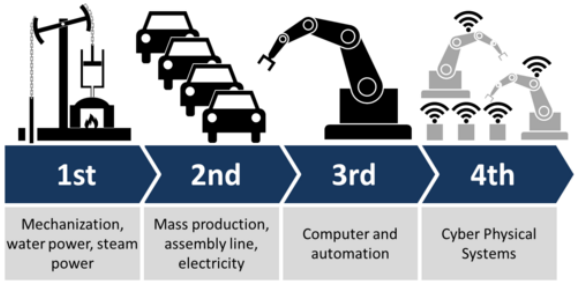
As internet revolutionized the connectivity of people, similarly IoT will transform the world into a smarter world where objects would communicate with each other. But to realize the full fledged vision of IoT, an efficient and secure medium is required which would ensure provisioning of reliable services. Security and privacy are the major issues of IoT applications and they need to be acknowledged. Therefore, we should pay more attention to the research issues for confidentiality, authenticity, and integrity of data in the IOT.

The structure of rest of this paper is as follows: Section II discusses the motivation behind the research, followed by Section III which describes the Security Aim and Goals of IoT. Further, Section IV provides the brief description of the possible Security threats to an IoT application..Finally, Section VI ends up with some conclusions and future research scope in IoT security construction.

II. Motivation

Motivation behind this study is the Fourth Industrial Revolution(Industry 4.0).In the First Industrial Revolution, water and steam power were used to mechanize production. In the Second Industrial Revolution, electric power was used to create mass production. In the Third Industrial

Revolution, electronics and information technology were used to automate production. Now a Fourth Industrial Revolution is building on the Third, i.e, the digital revolution which has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres. The possibilities of billions of people connected by mobile devices, with unmatched processing power, storage capacity, and access to knowledge, are unlimited. And these possibilities will be multiplied by unfolding technology breakthroughs in fields such as the Internet of Things, etc.



Source::https://www.linkedin.com/pulse/journey-40-industrial-revolution-majid-ali

There are many reasons to navigate to the next revolution i.e. Industry 4.0. Like, it is easier to make money today with fewer workers than it was 25 years ago. Setting up and running a company was an expensive business and required many workers. A company which makes its money out of a smart application requires less capital since it doesn't have to pay for the storage or transport in the way that usual companies do and incurs no extra costs virtually as the number of users increases. In the jargon of economics, the marginal costs per unit of output tend towards zero and the returns to scale are high. This gives an explanation for why tech entrepreneurs can get very rich very young. This builds the motive behind the study on Internet of Things and the concerns regarding the security and the privacy of the application.

III. Current Security Status

The expected growth of the global Internet of Things (IoT) market will lead to increased security risks as hackers are presented with a greater surface area to compromise. With the prominent rise of IoT comes huge amount of data, which can form appealing targets for malicious hackers. This, combined with IoT communicating frequently across a greater escalation of devices, opens up an increased risk of

cyber-crime. With any rapid technical revolution, such as IoT, security is often the last element to be considered. This, combined with the huge growth of cyber-crime and with lots of newly connected devices, opens up a world of new opportunities for hackers, many of which the end user will be completely unaware of. There are countless scenarios where this will be the case. Smart homes that are filled with connected devices are loaded with possibilities for hackers. Take a smart fridge for example, which will have access to the personal information and, possibly, the payment details of the user. If it's authorizing payments on the user's behalf, hackers can exploit this device and steal the user's credit card information. Another example is Smart buildings. As these premises are controlled by IoT, as opposed to office maintenance staff, these buildings will be vulnerable to hacks, be it to gain illegal entry or to steal company data.
Better security technologies will need to be developed to protect the IoT devices and platforms from both the information attacks as well as the physical tampering. The problem is that many "things" which make up the IoT use simple processors and operating systems may not support sophisticated security mechanisms.
Also devices will even need to be shielded from the challenges such as impersonation and "denial-of-sleep" attacks which are meant to drain batteries. Apart from the devices themselves, some communications will also be needed to be encrypted as well.

IV. Attacks on the IoT application

There are various potential security attacks that can be implemented on an IoT application under four distinct classes; Physical, Network, Software and Encryption attacks. An IoT system can be attacked physically, or attacked from within its network, or from applications on the system, and lastly from attacks on encryption schemes.

Physical attacks: Node Jamming, Physical Damage, Node Tampering, Social Engineering, Malicious Node Injection, Sleep Deprivation Attack, Malicious Code Injection on the Node.

Network attacks: Traffic Analysis Attacks, RFID Spoofing, RFID Cloning, RFID Unauthorized Access, Man In the Middle Attack, Denial of Service, Sinkhole Attack, Routing Information Attacks, Sybil Attack

Software attacks: Virus and Worms, Malicious Scripts, Spyware and Adware, Trojan Horse, Denial of Service

Encryption attacks: Man In The Middle Attack, Side Channel Attacks, Cryptanalysis Attacks

A. Physical Attacks

These kinds of attacks are focused on the hardware components of the IoT system and the attacker needs to be physically close or into the IoT system for the attacks to work.
What is more, attacks that harm the lifetime or functionality of the hardware are also included in this category. We will next explore these attacks.

1) Node Tampering

A sensor node can be damaged by the attacker, by physically replacing the entire node or part of its hardware or even electronically interrogating the nodes to gain access and alter sensitive information, such as shared cryptographic keys (if any) or routing tables, or impact the operation of higher communication layers .

2) RF Interference on RFIDs

A Denial of Service attack can be implemented on any RFID tag by creating and sending noise signals over the Radio Frequency signals which are used by the RFIDs for communication. The noise signals will interfere with the RFID signals hindering communication.

3) Node Jamming in WSNs

This is similar to the Radio Frequency Interference physical attack explained earlier for the RFIDs with the difference that this attack is based on the WSNs. The attacker can interfere with the radio frequencies of the wireless sensor nodes, jamming the signals and denying communication to the nodes. If the attacker manages to jam key sensor nodes he can successfully deny service of the IoT [1].

4) Malicious Node Injection

The adversary can physically deploy a new malicious node between two or more nodes of the IoT system, hence controlling all data flow from and to the nodes and their operation; this is also known as Man in The Middle Attack.

5) Physical Damage

The adversary can physically damage devices of the IoT network for his own gain. This kind of attack is an attack that deals with security of the area or building that hosts the IoT system. It differs from Node Tampering attack as in this situation the adversary tries to directly damage the IoT system with the purpose of impacting the availability of service.

6) Social Engineering

The attacker manipulates users of an IoT system, to extract private information or to perform certain actions that would serve his goals. This kind of attack is put under the physical attacks category because the attacker needs to physically interact with the IoT network users to achieve his goals.

7) Sleep Deprivation Attack

Most sensor nodes in the IoT system are powered by replaceable batteries and are programmed to follow sleep routines to extend their battery life. This attack, keeps the nodes awake which will result in a more power consumption, and will cause the nodes to shut down.

8) Malicious Code Injection

The attacker compromises a node by physically injecting it with malicious code that would give him access to the IoT system; e.g. imagine an attacker inserting a USB stick with harmful software (i.e. virus) onto the node. This would mean that the attacker could gain full control of the node or even control of the whole system.

B. Network Attacks

These attacks are centered on the IoT system network and the attacker does not necessarily need to be close to the network for the attack to work.

1) Traffic Analysis Attacks

An attacker can sniff out the confidential information or any other data flowing from the RFID technologies because of their wireless characteristics [2]. Also, in almost all of the attacks an attacker first tries to gain some network information before he employs his attack. This is done using sniffing applications like port scanning application, packet sniffer applications etc. [3].

2) RFID Spoofing

An attacker spoofs an RFID signals to read and record a data transmission from an RFID tag. Then the attacker can send his own data containing the original tag ID, making it appear to be valid, hence the attacker gains full access to the system pretending to be the original source [4].

3) RFID Cloning

An attacker clones an RFID tag by copying data from the victims RFID tag, onto another RFID tag. Although the two RFID tags have identical data, this method does not replicate the original ID of the RFID, making it possible to distinguish between the original and the compromised, unlike the event in the RFID spoofing attack.

4) RFID Unauthorized Access

Because of the lack of proper authentication mechanisms in the majority of RFID systems, tags can be accessed by anyone. This automatically means that the attacker can read, modify or even delete data on the RFID nodes [5].

5) Sinkhole Attack

The attacker lures all traffic from WSN nodes, hence creating a metaphorical sinkhole. This type of attack breaches the confidentiality of the data and also denies service to the network by dropping all the packets instead of forwarding them to the desired destination [6].

6) Man In the Middle Attack

The attacker over the network manages to interfere between two sensor nodes, accessing restricted data, violating the privacy of the two nodes by monitoring, eavesdropping and controlling the communication between the two sensor nodes [7]. Unlike the Malicious Node Injection from the Physical Attacks category, the attacker does not necessarily need to be physically there for this kind of attack to be successful, but relies solely on the network communication protocols of an IoT system.

7) Denial of Service

An attacker can bombard an IoT network with more traffic data that it can handle which can result in a successful Denial of Service attack.

8) Routing Information Attacks

These are direct attacks that the adversary by spoofing, altering or replaying routing information can complicate the network and create routing loops, allowing or dropping traffic, sending false error messages, shortening or extending source routes or even partitioning the network; e.g. Hello Attack and Black hole Attack.

9) Sybil Attack

A malicious node (i.e. Sybil Node), is a single node that claims the identities of a larger number of nodes, and impersonating them. This kind of attack leads to false information being accepted by the neighboring WSN nodes; e.g. imagine a WSN voting system where one Sybil node votes more than once [8], or a Sybil node being selected as part of a routing path.

C. Software Attacks

Software attacks are the main source of security vulnerabilities in any computerized system. Software attacks exploits the system by using Trojan horse programs, worms, viruses, spyware and malicious scripts that can steal information, tamper with data, deny service and even harm the devices of an IoT System.

1) Phishing Attacks

The attacker gains access to confidential data by spoofing the authentication credentials of a user, usually through infected emails or phishing web sites .

2) Virus, Worms, Trojan Horse, Spyware and Aware

An adversary can infect the system with malicious software Resulting in a variety of outcomes; stealing information, Tampering data or even denial of service [9]

3) Malicious Scripts

Usually the IoT network is connected to the Internet. The user that controls the gateway can be fooled into running executable active-x scripts which could result in a complete system shut down or data theft [9].

4) Denial of Service

An attacker can execute DoS or distributed denial of service DDoS attacks on the affected IoT network through the application layer, affecting all users in the network. This

kind of attack can also block the legitimate users from the application layer giving full application layer access to the attacker; databases and private sensitive data.

D. Encryption Attacks

These attacks are solely based on breaking the encryption scheme being used in an IoT system.

1) Side channel Attacks

Using particular techniques (i.e. Timing, Power, Fault and Electromagnetic Analysis) on the encryption devices of an IoT system, the attacker can retrieve the encryption key being used for encrypting and decrypting data.

2) Cryptanalysis Attacks
These attacks assume the possession of cipher text or plaintext and their purpose is to find the encryption key being used by breaking the encryption scheme of the system. Examples of cryptanalysis attacks on IoT systems include Known-plaintext attack, Chosen-plaintext attack, Chosen Ciphertext attack, and Ciphertext-only attack.

3) Man In the Middle Attack

When two users of an IoT system A and B, exchange keys during a challenge-response scenario, so as to establish a secure communication channel, an adversary positions himself between them on the communication line. The adversary then intercepts the signals that A and B send to each other and attempt to interfere by performing a key exchange with A and B separately. The adversary will then be able to decrypt/encrypt any data coming from A and B with the keys that he shares with both of them. Both A and B will think that they are talking with each other.

V. Literature Survey

Although security challenges and security mechanisms have been widely studied in various fields (e.g., WSNs), current IoT research has not comprehensively investigated how to provide a proper classification of security challenges.

The first paper [1] that is, "A survey on jamming attacks and countermeasures in WSNs." by A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, provides a general overview of the critical issue of jamming in WSNs and cover all the relevant work, providing the interested researcher pointers for open research issues in this field. It highlights the characteristics of contemporary WSNs, that make them susceptible to jamming attacks, along with the various types of jamming which can be exercised against WSNs. Common jamming techniques and an overview of various types of jammers are reviewed and typical countermeasures against jamming are also analyzed. The key ideas of existing security mechanisms against jamming attacks in WSNs are presented and open research issues, with respect to the defense against jamming attacks are highlighted.

The second paper [2] i.e. "RFID as an enabler of the internet of things: issues of security and privacy." by B. Khoo, discusses the current RFID usage issues and conduct a threat analysis of the RFID system components then identify issues/risks and elucidate how these issues can be resolved or risks can be mitigated.

In the third paper [3] i.e. "Content sniffing attack detection in client and server side: A survey." by B. S. Thakur, and S. Chaudhary, is a thorough study of security problems in IoT is presented and classify possible cyber-attacks on each layer of IoT architecture. It also discusses challenges to traditional security solutions such as cryptographic solutions, authentication mechanisms and key management in IoT. Device authentication and access controls are an essential area of IoT security, which is not surveyed so far.

The fourth paper [4] which is "Classification of RFID attacks." by A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, develops a structural methodology for risks that RFID networks face by developing a classification of RFID attacks, presenting their important features, and discussing possible countermeasures. The goal of the paper is to categorize the existing weaknesses of RFID communication so that a better understanding of RFID attacks can be achieved and subsequently more efficient and effective algorithms, techniques and procedures to combat these attacks may be developed.

The fifth paper [5] i.e. "Internet of Things: Architecture and Security." by R. Uttarkar, and R. Kulkarni, analyzes the security issues and challenges and provides well defined security architecture as a confidentiality of the user's privacy and security which could result in its wider adoption by masses.

Wireless Sensor Network (WSN) is being emerged as a prevailing technology in future due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks. Unattended installation of sensor nodes in the environment causes many security threats in the wireless sensor networks. There are many possible attacks on sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Sinkhole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. Once sinkhole attack has been implemented and the adversary node has started to work as network member in the data routing, it can apply some more threats such as black hole or gray hole. Ultimately this drop of some important data packets can disrupt the sensor networks completely. The sixth paper [6] i.e. "Detecting Sinkhole attack in wireless sensor network." by V. Soni, P. Modi, and V. Chaudhri ,has presented some countermeasures against the sinkhole attack.

The seventh research paper [7] i.e. "Cloud Computing: Security Issues and Research Challenges." by R. P. Padhy, M. R. Patra, and S. C. Satapathy, outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as

well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

The eighth paper [8] i.e. "The sybil attack in sensor networks: analysis & defenses." by J. Newsome, E. Shi, D. Song, and A. Perrig, systematically analyzes the threat posed by the Sybil attack to wireless sensor networks. It demonstrates that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. It establish a classification of different types of the Sybil attack, which helps to better understand the threats posed by each type, and better design countermeasures against each type. We then propose several novel techniques to defend against the Sybil attack, and analyze their effectiveness quantitatively.

In the ninth paper [9] i.e. "Security Challenges in the IP-based Internet of Things." by H. Tobias, et al , the applicability and limitations of existing Internet protocols and security architectures in the context of the Internet of Things is discussed. First, it gives an overview of the deployment model and general security needs and then present challenges and requirements for IP-based security solutions and highlight specific technical limitations of standard IP security protocols.

VI. Conclusion

IoT has been a major research topic for almost a decade now, where physical entities would interconnect using existing network technologies to exchange information. Due to its high-speed advancement many threats in security and privacy exists, which hinder its development. This paper explored the security issues which should be addressed for a secure IoT system, and classified its security challenges and issues using a new unique classification method consisting of four classes of attacks; Physical, Network, Software, and Encryption Attacks. Furthermore, future directions for security for IoT were discussed. This classification could be used as a framework to categorise attacks, as well as to guide the secure deployment of IoT systems. As future work, we aim to investigate the interaction between heterogeneous IoT devices and its impact on security. Further, we aim to investigate the security for IoT systems in detail.

VII. References

[1] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs."Communications Surveys & Tutorials, IEEE 11, no. 4 (2009): 42-56.
[2] B. Khoo, "RFID as an enabler of the internet of things: issues of security and privacy." In Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, pp. 709-712. IEEE, 2011.
[3] B. S. Thakur, and S. Chaudhary, "Content sniffing attack detection in client and server side: A survey." International Journal of Advanced Computer Research (IJACR) 3, no. 2 (2013): 10.
[4] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks." Gen 15693 (2010): 14443.
[5] R. Uttarkar, and R. Kulkarni, "Internet of Things: Architecture and Security."
[6] V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network." International Journal of Application or Innovation in Engineering & Management 2, no. 2 (2013).
[7] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS) 1, no. 2 (2011): 136-146.
[8] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses." In Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259-268. ACM, 2004.
[9] H. Tobias, et al. "Security Challenges in the IP-based Internet of Things." Wireless Personal Communications 61, no. 3 (2011): 527-542.