THREATS IN IOT AND SECURITY BY INTEGRATED IOT DEVICES USING BLOCK CHAIN :A SURVEY

[1] G. Rekha
Assistant Professor
Kuppam Engineering College
KES Nagar,Kuppam-517425

[2] Y.Suneetha
Assistant Professor
Kuppam Engineering College
KES Nagar,Kuppam-517425

Abstract: Internet of Things is a newly-visible technology having the ability to change the way we live. Many IoT services can make our daily life easier, smarter, and even safer. IoT is growing rapidly in the field of telecommunications. Numerous IoT services can make our daily life easier and even smarter. However, all those benefits can come of huge risks of privacy loss and security issues. To secure the IoT devices, many research works have been conducted to encounter those problems and find a better way to eliminate or to reduce those risks. In this paper we presented a survey which consists of three pieces/parts. The first part will explore the limitation of IoT devices which increases the security and privacy issues. The second one will discuss the present classification of IoT attacks. Third part will explain about threats to the Internet of things security. Finally, an integration of IoT devices which improves security using Block Chain.

KEYWORDS: Block Chain, Internet of Things (IoT), Distributed Denial of Service (DDoS), Security, Privacy.

I.INTRODUCTION

INTERNET OF THINGS (IoT) is a collection of "things" embedded with electronics, software, sensors, mechanical pushing-pulling devices, and connected via the Internet to collect and exchange data with each other. The IoT devices have sensors and processing power that enable them to be sent out and used in many (surrounding conditions). Figure 1 presents a variety of common IoT computer programs, including smart home, smart city, smart grids, medical and healthcare equipment, connected vehicles, etc. The fast growth of the number of IoT devices used is (described a possible future event) to reach 41 billion in 2020 with an $8.9 trillion market [1] as stated in the 2013 report of the International Data Corporation (IDC). The difference between IoT and the usual Internet is the (not being there; not being present) of Human role. The IoT devices can create information about person's behaviors, carefully study it, and take action [2]. Services done by IoT computer programs offer a great benefit for human's life, but they can come with a huge price (thinking about/when one thinks about) the person's privacy and security protection.

Figure 1: Internet of Things and its applications

With recent development in communication technologies the IoT is expected to help widespread sensing and (producing a lot with very little waste) useful thing/valuable supply management in applications such as smart power grids, smart spaces, smart cities, industry automation, health care, etc. to name a few [1] shown in Figure 1. A high-level summary of IoT based systems is shown in Figure 1 where different IoT de- bad behaviors/crimes (e.g. sensors and mechanical pushing-pulling devices) communicate with a (controlled by one central place) server through a communication network. It is guessed that by 2020, between 50-100 billion things (objects) will be connected to the Internet [2]. Due to the large size of the network and the sensitive nature of the data these devices produce, security is a serious concern for some IoT applications. The IoT devices can create information about individual's behaviors, analyze it, and take action [2]. Services provided by IoT applications offer a great benefit for human's life, but they can come with a huge price considering the person's privacy and security protection. So, in order to enable secure communication between a large number of devices, new security ways of doing things and rules of conduct are needed/demanded that can serve/be controlled by the (detailed descriptions of exactly what is required) of ordinary as well as new IoT devices.

In this survey paper, we explore the IoT security and privacy privacy issues in four aspects. The first part presents the limits of IoT devices and their solutions. The second part discusses the classification of existing IoT attacks. Third part will explain about threats to the Internet of things security. Finally an integration of IOT devices using block chain.

II.IOT DEVICE LIMITATIONS

Why is it very hard to secure and apply security features to IoT as those used in traditional Internet? Trappe et al. [4] presented the issue of IoT restrictions, and their effects. The two main limits are the battery capacity and computing power.

A. Battery Life Extension

Many of the IoT devices are utilized in the environment where charging is not available, they have a limited energy to do the designed function and heavy security instructions can drain the devices useful things[4]. Three possible approaches can be used to eliminate/reduce this issue. The first is to use the minimum security needed things on the device, which is not recommended especially when dealing with sensitive data. The second approach is to increase the electrical storage device capability. However, most IoT devices are designed to be lightweight and in small size. There is no extra room for a larger electrical storage device. The final approach is to harvest energy from valuable things from nature (e.g., light, heat, vibration, wind), but this type of approach would require an upgrade to the hardware and significantly cost-effective.

B. Lightweight Computation

The paper [4] said that conventional cryptography may not work on IoT systems, since the devices have limited memory space which can't handle the computational and storage requirements of advanced cryptography. To support security for the IOT devices, the authors suggested reusing existing functions. One way is using physical layer authentication by applying signal processing at the receiver side to verify whether a transmission came from the expected transmitter in the expected location. The another method is analog characteristics of a transmitter can be used to effectively encode analog information. This way of providing authentication has little energy overhead because it takes advantage of radio signals.

III. CLASSIFICATIONS OF ATTACKS

The IoT architecture is given in Figure 2. According to many researchers [7], IoT technology works on three layers:

1.Perception Layer

2.Network Layer

3.Application Layer

Perception Layer involves various types of data sensors like RFID, Barcodes or any other sensor network[4]. The aim of this layer is to obtain information from the environment by using sensors and then send it to the network layer. The aim of network layer is to transmit the data collected from the perception layer to any specific information processing system through internet, mobile network or any other kind of reliable network[8]. The aim of the IoT is developing smart environment is accomplished at the application layer.The security of IoT is a big challenge because of complexity, heterogeneity and a large number of interconnected resources. The adversary can perform the attack on IoT system by damaging or tampering some node i.e. physical vulnerability, or from within its network by using faults in routing protocol and other network related protocol, or by using malicious program and by breaking encryption strategy i.e. encryption attack.

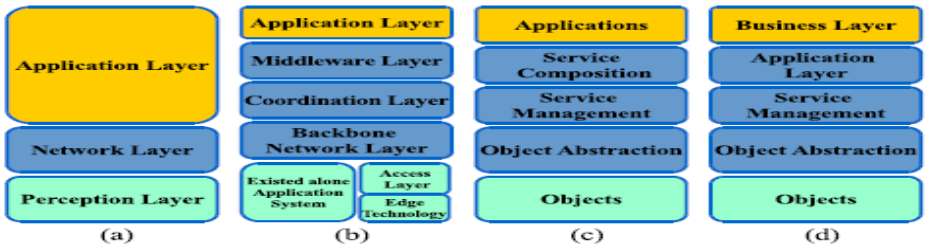


Figure 2: IOT Architecture

Andrea et al come up with a new classificationof IoT devices attacks[5] presented in four types which are given in Figure 3 as follows

A. Physical Attack

B. Network Attack

C.Software Attack

D.Encryption Attack.

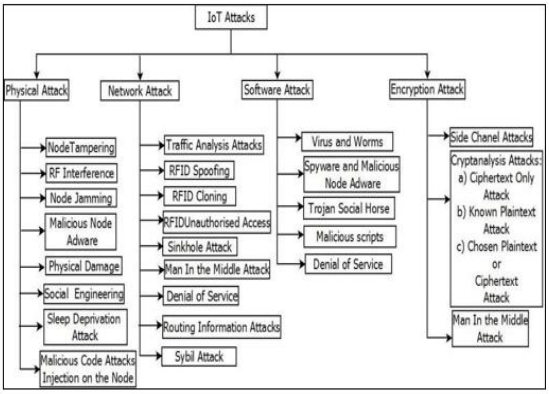


Figure 3: IoT and its Security Attacks

A.Physical Attack

Physical attacks[8] are a type of cryptanalysis, or the analysis of information systems in order to discover the hidden aspects of devices and systems using their implementation properties. Fault Injection is the force used to change the physical behavior of the running device to discover additional security information or ways into the system. Physical attack and fault injection research is critical because it is a preferred low cost attack method used by both black hats to discover new IoT/hardware/software attack vectors, as well as by white hats to help discover and address these vulnerabilities early in the design cycle before the get to market.

From physical attack, malicious node injection attack has been the dangerous attack. Since it is not only stopping the services but also modify the data. The physical attack is performed when the attacker is in a close distance of the device. The physical attack surface is the totality of the security vulnerabilities in a given system that are available to an attacker in the same location as the target.

B.Network Attack

network attacks consist of manipulating the IoT network system to cause damage[8]. The software attacks happen when the IoT applications present some security vulnerabilities that allow the attacker to seize the opportunity and harm the system. From network attack, sinkhole attack is the most risky attack. It not only attracts all the traffic towards the base station, but also the attacker can initiate other threats such as selective forwarding, altering or dropping the packets.

C.Software Attack

Andrea et al[5] presented that the software attacks happen when the IoT applications present some security vulnerabilities that allow the attacker to seize the opportunity and harm the system.From software attack, we select worm attack as most unsafe.

Worms are probably the most destructive and dangerous form of malware on the internet. It is the self-replicating program which harms the computer by using security holes in networking software and hardware. It can delete the files in system, steals the information like passwords, they can also change the passwords without your notice, it causes the computer lockouts, etc. Security researchers have created an experimental IoT worm that can spread on its own to nearby compatible smart devices, causing havoc inside a modern smart city by allowing an attacker to jam WiFi connections, disturb the electric grid, or brick devices making entire critical systems inoperable.

D.Encryption attack

Encryption attacks[2] consist of breaking the system encryption. This kind of attacks can be done by side channel, cryptanalysis, and man-in-the-middle attacks. These attacks depend on destroying encryption technique and obtain the private key.

1.Side-channel Attacks: The attacker uses the side channel information that is emitted by encrypting devices. It is neither the plaintext nor the cipher text, it contains information about power, thetime required to perform theoperation, faults frequency, etc. Attacker uses this information to detect the encryption key.

2.Cryptanalysis attacks: These attacks [5] are focused on the cipher-text and they try to break the encryption, i.e. find the encryption key to obtain the plaintext. Examples of cryptanalysis attacks include cipher-text only.

3.Man in the Middle Attacks*:* When two users are interchanging the key the attacker intercepts the communication and obtains the key.

IV. Threats to the IOT Security

Potential attacks[5] against the Internet of Things into three primary categories based on the target of the attack—attacks against a device, attacks against the communication between devices and masters, and attacks against the masters. To protect end users and their connected devices, we need to address all three of these IoT attacks.

Attacks Against IoT Devices

To a potential attacker, a device presents an interesting target for several reasons[8]. First, many of the devices will have an inherent value by the simple nature of their function. A connected security camera, for example, could provide valuable information about the security posture of a given location when compromised.

Attacks Against Communications

A common method of attack[5] involves monitoring and altering messages as they are communicated. The volume and sensitivity of data traversing the IoT environment makes these types of attacks especially dangerous, as messages and data could be intercepted, captured, or manipulated while in transit. All of these threats jeopardize the trust in the information and data being transmitted, and the ultimate confidence in the overall infrastructure.

Attacks Against the Master of Devices

For every device or service in the Internet of Things, there must be a master. The master's role is to issue and manage devices, as well as facilitate data analysis. [8]Attacks against the masters – including manufacturers, cloud service providers, and IoT solution providers – have the potential to inflict the most amount of harm. These parties will be entrusted with large amounts of data, some of it highly sensitive in nature. This data also has value to the IoT providers because of the analytics, which represent a core, strategic business asset—and a significant competitive vulnerability if exposed.

V.The Blockchain Approach

Blockchain, the "distributed ledger" technology that underpins bitcoin, has emerged as an object of intense interest in the tech industry and beyond [11]. Blockchain technology offers a way of recording transactions or any digital interaction in a way that is designed to be secure, transparent, highly resistant to outages, auditable, and efficient; as such, it carries the possibility of disrupting industries and enabling new business models. The technology is young and changing very rapidly; widespread commercialization is still a few years off. Nonetheless, to avoid disruptive surprises or missed opportunities, strategists, planners, and decision makers across industries and business functions should pay heed now and begin to investigate applications of the technology.

Blockchain

Blockchain is a database that maintains a continuously growing set of data records. It is distributed in nature, meaning that there is no master computer holding the entire chain. Rather, the participating nodes have a copy of the chain. It's also ever-growing — data records are only added to the chain [11].

A blockchain consists of two types of elements:

- **Transactions** are the actions created by the participants in the system.
- **Blocks** record these transactions and make sure they are in the correct sequence and have not been tampered with. Blocks also record a time stamp when the transactions were added

The Blockchain and IoT

Blockchain technology is the **missing link** to settle scalability, privacy, and reliability concerns in the Internet of Things. Blockchain technology can used in tracking billions of IOT devices, enables the processing of transactions and coordination between devices; This decentralized approach would eliminate single points of failure, creating a more resilient ecosystem for devices to run on. The cryptographic algorithms used by blockchains, would make consumer data more private.

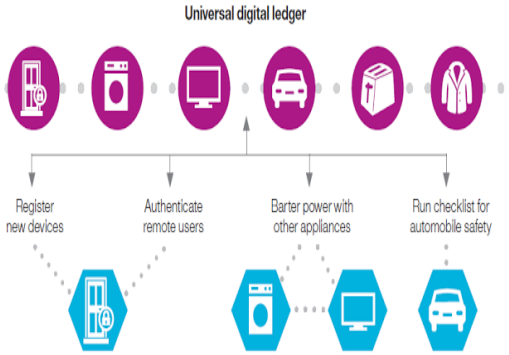


Figure 4:Distributed transaction ledger for various IOT Transaction

The ledger is tamper-proof and cannot be manipulated by malicious actors because it doesn't exist in any single location, and man-in-the-middle attacks.Figure 4 explains the transaction ledger for various IoT transactions .Blockchain makes trustless, peer-to-peer messaging possible and has already proven its worth in the world of financial services through cryptocurrencies such as Bitcoin, providing guaranteed peer-to-peer payment services without the need for third-party brokers.

By leveraging the blockchain, IoT solutions can enable secure, trustless messaging between devices in an IoT network. In this model, the blockchain will treat message exchanges between devices similar to financial transactions in a bitcoin network.

One of the most exciting capabilities of the blockchain is the ability to maintain a duly decentralized, trusted ledger of all transactions occurring in a network. This capability is essential to enable the many compliance and regulatory requirements of industrial IoT applications without the need to rely on a centralized model.

Selection of blockchain Technology for IoT Security

Blockchain technology can help secure IoT devices. IoT devices can be configured to communicate with private blockchain nodes in the cloud over a secure API [12]. Blockchain technology can improve the security of an IoT system which allows IoT devices to securely discover each other, encrypt machine-to-machine transactions using distributed key management techniques. Based on the potential architectural patterns detailed in this report, an IoT device will communicate with a blockchain transaction node via an API, allowing even constrained devices to participate in the blockchain service.

Dorri et al[13] presented that, to ensure security, care should be taken during the bootstrapping of an IoT device onto a particular blockchain service[11,13]. The IoT device must first be provisioned with credentials that can be used to prove authorization in order to be added to a transaction node. This credential provisioning must be done in a secured environment that safeguards against threats of a particular IoT device ecosystem. Five features to be consider when securing the IoT using blockchain technology:

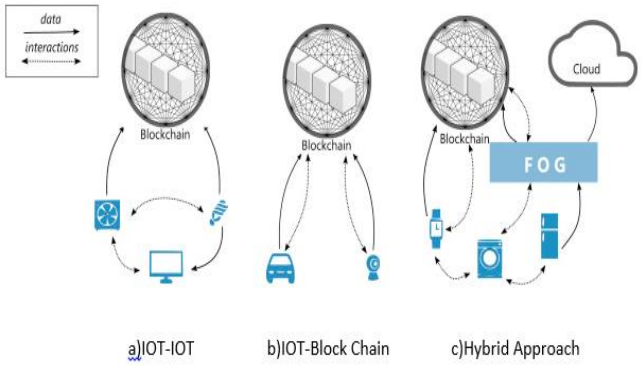
1.Scalable IoT discovery
2. Trusted communication
3. Message authentication/signing
4. IoT configuration and updates
5. Secure firmware image distribution and update

Scalable IoT discovery Smart cities and large enterprise IoT deployments will result in the activation of potentially thousands or tens of thousands of IoT devices that must work together. Figure 5 describes the Blockchain IoT interaction. Often, these devices will coordinate with each other in autonomous machine-to-machine transactions. The devices must also be able to discover legitimate peers and services with which to interact. IoT systems can take advantage of scalable IoT discovery using both public and private blockchain implementations. Within Bitcoin for example, a set of hard-coded Named DNS seeds provides bootstrap services for new users and devices. These DNS Seeds can be preconfigured within an IoT device. IoT devices query these addresses and are provided with the IP address of a full node. The IoT device then registers itself into a node and requests a list of other IoT devices on the network. When provisioned, the IoT device can begin peer-to-peer communications while promulgating peer discovery information to neighbors across the network. The preconfiguration (hard-coding) of the Named DNS Seed addresses reduces the ability to perform a man-in-the-middle (MITM) attack. IoT devices receive information from multiple DNS Seeds before choosing a node to enroll within. DNS Sec must be used to secure the name resolution of root servers and mitigate DNS spoofing attacks. Named DNS Seed addresses should be hard-coded into the firmware [11] .

This paper provides a way to secure firmware image distribution and update. A private blockchain service can also support the bootstrap and enrollment of IoT devices onto a network[13]. Transaction nodes will authenticate the IoT devices prior to providing a trusted node list. 18 credentials that can include the following:

1.Security credentials installed on or internally self-generated in the IoT device during setup must be generated and provided using a safe process that could be part of blockchain implementation.

2.Credentials provided by the owner or installation technician of the IoT device would initialize the device enrollment into a security server to get specific credentials for the IoT. In either case, the enrollment process must be enforced to ensure only legitimate IoT devices can be added to the blockchain service.



4) BlockChain IOT Interactions

All communication described must be authenticated and encrypted to ensure confidentiality and integrity. For further information on the ability to register device identities onto the blockchain, visit the Trusted IoT Alliance to review the blockchain APIs developed for registering thing identities on the blockchain.

Conclusion

In this survey, we have presented the security issues in IoT applications and systems. We discussed the limitations of IoT devices in battery and computing resources, and possible solutions for battery life extension and lightweight computing.With the development of IoT, many kinds of attacks also have been invented to breach the security of IoT devices. Researchers have proposed different solutions on these attacks to tackle it.In addition we have presented the blockchain technology for IOT security. It will ensure proper security by ensuring the privacy and protection of data at all levels. In addition, blockchain can help resolve scalability issues and provide an effective functioning of the system as well. .However,IoT Technology will play an increasingly important role in our society for the future in both military and civilian context including the internet of drones and internet of battle field things.

References

[1] IoT Analytics, "Why the internet of things is called internet of things: Definition, history, disambiguation," https://iot-analytics.com/internet- of-things-definition/, 2014.

[2] Brian Lam and Cynthia Larose, "How did the internet of things allow the latest attack on the internet?" https://www.privacyandsecuritymatters.com/2016/10/how-did-the- internet-of-things-allow-the-latest-attack-on-the-internet/, 2016.

[3] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015.

[4] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan 2015

[5] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, July 2015, pp. 180–187.

[6] T. Yousuf, R. Mahmoud, F. Aloul, I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures", International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015.

[7] L. Li, "Study on security architecture in the Internet of Things," International Conference on Measurement, Information and Control (MIC), pp. 374-377,Harbin, China, 2012,.

[8] Kaur, Damandeep, and P. Singh, "Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack",International Journal on Network Security 5.1 (2014): 62.

[9] L. Li, "Study on security architecture in the Internet of Things," International Conference on Measurement, Information and Control (MIC), pp. 374-377,Harbin, China, 2012,.

[10] Talkin Cloud, "Iot past and present: The history of iot, and where it's headed today,"

[11] Compton,J. How Blockchain Could Revolutionize the Internet of Things. *Forbes*

[12] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010

[13] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, pp. 618–623, IEEE, Kona, HI, USA, March 2017.