IoT Security and Privacy Issues

I. INTRODUCTION

The Internet of Things (IoT) simply is a collection of many connectable objects (nodes) that can communicate and share information to accomplish common tasks. Objects can be a person, mobile phones, home appliances, doors, cars, animals or anything else you can imagine. Each object is attached to a sensor that enables it to connect with the environment. IoT connects personal, business, industrial, and public-sector devices to each other, where the information can be sorted, analyzed, and stored. It has many applications in transportation, healthcare, energy production, and distribution. ITU-T defines IoT as: "Global infrastructure for the society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.". IoT represents a new revolution of the Internet and it will change our daily lifestyle. It makes intelligent devices around us perform our daily tasks. In the future, almost all the objects around us will connect to the internet to communicate. Smart home, smart office, smart car and smart cities all are new words appeared with IoT. According to Gartner , the number of IoT connected devices will increase by 2020 from about 25 billion devices to be more than 50 billion devices. This huge size network with heterogeneous nature creates new security issues and risks which increase the targeted surface and allow for attackers to reach more of personal information from the IoT network that will facilitate the attacking process. IoT nodes communicate with each other and connect to the internet with no standard rules or regulations. This raises many security and privacy concerns. At the same time, its huge size and heterogeneous nature create more challenges for proposed solutions.

The next section provides a brief introduction to the concept ofIoT and its architecture, then an overview of IoT security at each architecture layer is discussed in section 3. Section 4 highlights IoT security requirements, challenges, and some proposed solutions for IoT security challenges. Section 5 provides an overview of the privacy issue in IoT then a discussion and conclusion.

II . IOT OVERVIEW

A. Evolution

Internet of Things term was proposed in 1999 by Kevin Ashton at Massachusetts Institute of Technology and IoT began to spread in markets, but it was limited in use due to low performance of the network. Sristava in 2011 announced that with RFID, things tagging can be done using other technologies such as near field communication (NFC) and QR codes. By 2020 IoT devices will be more than 50 billion. IoT is a new generation of the internet where communication goes beyond machine-to- human to a machine –to- machine. It is a network of objects such as mobile phones, doors, wearable devices, cars, TV and more. Each device embedded with sensor and technology like radio frequency identification (RFID).

IoT transforms the communication model to M2M communication model. IoT introduced a broader change to the computing vision, business, health-care sector, industrials and our daily activities. The current industrial aim is to "connect the unconnected" which mean every single device around us will be able to connect and exchange information. However, many IoT devices with heterogeneous nature and high computational power make them an easy target for attackers. Security is one of the major problems faces the IoT growth . A survey showed that 71% of participants agree that security concerns have affected the decision of customers of IoT products .

B. Architecture

IoT makes an interconnection between various heterogeneous objects, so there is a need for a flexible layered architecture. There is no uniform IoT architecture, but the basic IoT model has 3-layer architecture, including the application layer, the network layer, and the perception layer. Each IoT layer differentiates by its functions and technologies attached with, so each layer has security issues associated with it . The layers are:

1. **Perception Layer**
   This layer is known as "sensors layer ". This layer identifies, gathers, processes data and then send it to the network layer. It also represents a sensor network and shows IoT node cooperation in short-range networks. It mostly uses Radio Frequency Identification (RFID) technology, GPS, and sensors [7].
2. **Network Layer**
   This layer works on the data routing or data forwarding to different hubs over IoT and Internet. Switching, cloud computing platforms, routers and internet gateways are essential parts of the network layer. It uses some technologies such as 2G/3G, Satellite Access, LTE, WIFI, Bluetooth, and ZigBee. Gateways at this layer work as the interface between nodes by collecting, filtering, and transmitting data between sensors .
3. **Application Layer**
   The purpose of IoT is clearly achieved at this layer by providing various smart environment applications. Smart home, smart office, smart city, and smart transportation, etc. are typical applications of IoT. IoT has a personalapplication such as applications of smart wearable devices or mobile app and industrial applications such as autonomous vehicles applications .

Confidentiality, integrity, and availability are general security goals in any system, it is applied also to IoT. IoT has many limitations which make security a big challenge, such as the heterogeneous nature of the nodes that has access to the internet with less embedded protection device . This section provides an overview of security issues at each IoT layer, then discusses IoT security requirements and threats and some proposed solutions for IoT security.

B. Security Issues at each Layer

1. Perception Layer

Usually, the IoT nodes are placed out-door and exist in an environment that exposes them to physical attacks and to natural accidents as well. These conditions made IoT nodes easy targets for physical attacks, for example, an attacker can tamper with a device element once he gets a physical accessto it. In addition, IoT has a dynamic nature where they needto be movable in many applications which increase the risk of such attacks. Moreover, this layer usually consists of sensors with RFIDs and wireless sensor networks which has many security problems such as information leakage, replay attacks, cloning attacks and man-in-the-middle attacks. Also, the low storage capacity with limited computation capability, make these nodes vulnerable to many types of attacks. Examples of such attacks are the replay attack which can easily exploit the confidentiality of this layer by spoofing or replaying device information identity. Also, timing attack where the attacker obtains the encryption key by analyzing encryption time. Malicious data in this layer can be generated by attacker nodes which threaten the data integrity and increase the risk of DoS attack. Most security issues at this layer can be solved by encryption, stenography, access control and authentication to confirm sender identity.

1. Network Layer

This layer usually is a target for data eavesdropping, DoS attacks, illegal access, destruction, viruses attack, Man-in-the-Middle etc. Attackers can analyze the traffic and eaves dropping to attack the network confidentiality and privacy. The remote access mechanisms of IoT and data exchange increase probability of such attacks. The key exchange mechanism must be in a high-security manner to protect it from any attacker. Communication in IoT environment introduces new security issues which are not common in theInternet. Traditional internet communication is between human and machines, while in IoT the communication is between machines. These machines do not follow standard security protocols for communication and exchange a lot of sensitive information. Network attackers can gain more information about the users from his IoT devices and use that information for criminal activities. In IoT, the object protection has important as well as the network protection. Current network protocols produce efficient protection mechanisms, however, they do not cover the IoT heterogeneous nature. Objects must be able to know the current network state and respond to any abnormal behaviors that may affect their security. Good protocols and software can help to achieve this level of protection .

2. Application Layer

There are many issues at the security of application due to the lack of standards that manage the interaction and the applications development process for applications. Applications with different authentication mechanisms are difficult to confirm authentication and data privacy. Traffic management is the responsibility of this layer, which makes it a target for DoS attack. Also, the great number of connected devices and generated data can create overhead in data analysis applications that in turn affects the service availability. The different user interaction with the application in IoT must be considered when designing the applications as well as the amount of data that will be generated .

D. General Security Requirements and Challenges in IoT

The main security requirements of IoT are discussed from different aspects by. IoT security requirements can be summarized in five main requirements as shown in the table1. Satisfying these requirements is a huge challenge due to the limitations associated with IoT devices with regards to their capacity and capability to implement traditional security solutions.

In addition, there are more challenges facing the achievement of IoT security requirements summarized as follows:

- **Date Volume:** Even though most of IoT applications use narrow communication channels, there are many IoT systems that have a chance of requiring a large amount of data at the central network .
- **Constraints in resources:** Most nodes in IoT have low storage and processing capacity so they usually have low-bandwidth communication channels which limit the use of some security techniques such as public key encryption algorithm .
- **Protection**: Since most of RFID systems have a weak authentication mechanism, it is easy to track tags and find objects identification. The invader will be able to read data, modify and even delete data .
- **Scalability**: IoT composed of a massive number of nodes and it expands with time. Hence, its security mechanism should be scalable .
- **Autonomic control:** Nodes in IoT should be able to make connections with each other and configure themselves to adjust at the platform. So, it must have some mechanisms and techniques such as self-configuring, self-management and self-healing all that automation make IoT need more control with security.

B. Some proposed solutions for IoT security

There have been some studies aiming to improve IoT security and to propose solutions to address security issues. Tahir and et al. in proposed ICMetric framework for securing IoT based on cryptography keys.

The ICMetric technology adds an additional layer of cryptographic schemes to solve problems related to key theft, which can be used for preventing unauthorized access. ICMetric technology is integrated into a healthcare environment, for an encryption that allows for the safe and secure use of electronic devices, which is a crucial requirement of IoT based healthcare applications. ICMetric technology also provides protection of data stored on and transmitted between the devices. Liu et al. in proposed solution serve IoT security based on the biological immune system. The proposed solution uses dynamic defense frame of the internet of thing security, where static security strategies could be unsuitable. The circular defense proposed with five links: security threat recognition, risk computation, security responses, security defense, and finally defense strategy formulization. The link in the frame is correlated with relative data of IoT security. Researcher simulated the real IoT platform by immunity-based antigen and in real IoT detector. They are emulating the mechanisms which are used to recognize pathogens in biological systems. Zhou and Chao

developed a security architecture for media-aware traffic, they designed and evaluated the traffic management scheme. The media-aware traffic security architecture (MTSA) fulfills the security requirements for multimedia communication, computation, and IoT service. Rose [18] described physically unclonable functions (PUFs) as an example of the implementation of security primitives and protocols for IoT devices. He described that in the IoT environment, the PUF has the potential to provide security enhancements in the form of robust authentication or secret key generation. Lessa dos Santos establish an architecture to let IoT limited devices able to "Datagram Transport Layer Security (DTLS)" with authentication to communicate with devices on the Internet.

This security architecture for IoT is based on IoT Security Support Provider (IoTSSP), which is a third-party device, also on two mechanisms for 6LoWPAN Border Router (6LBR) to redirect the DTLS handshaking to the IoTSSP. Zegzhda and Stepanova propose a solution that improves IoT security using topological sustainability to solve security threats that aimed to disruption, humiliating or destroying any components or services in the IoT. The aim is to maintain IoT security using topological sustainability by preserve adaptive d-regular graph topology and consider different internet of things requirements such as restrict computation resources at IoT devices. Raza implemented Scalable Security with Symmetric Keys, which introduce a highly scalable and flexible key management scheme for DTLS security standard for resources-constrained IoT devices.

IoT Privacy Issues

Privacy in IoT defined by the Internet security glossary as (DRM) system is a good method that can be used to control exchanged data rights and defend against illegally processing. DRM works on the base of devices trusted and secure to be effective.

The permission and awareness of data owner must be obtained before processing or even dealing with personal data. User notification helps to avoid improper use of private data and sensitive information .

"the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others".

In IoT, the network of devices tries to gain data from the environment, then broadcast it with some events to the server that has applications. During all that steps, privacy must be managed, in the device, storage, communication and while processing. The privacy with the protection of sensitive information in IoT was identified as one of the critical issues that need to be addressed .

A. Device Privacy

Sensitive information in IoT could be targeted when unauthorized access happens in hardware or software. For example, an invader able to re-program a camera to make it sends information not to the authorized server only, but to invaders too.

To provide the privacy in devices, there are many issues must be addressed, like device location privacy which can be achieved by Multi-Routing Random Walk Algorithm for Wireless Sensor Network (WSN), protecting the identification of device nature that can be achieved by adding noise and protecting the sensitive information even in case of device theft by using Quick Response Code technique.

B. During Communication Privacy

Data confidentiality when data being transmitted through network channels commonly achieved using encryption techniques. Encryption in some cases adds data to packets to provide tracing property. Communication Protocol for security can provide some solutions for privacy. Pseudonyms can be used during communication for encryption that may help to decrease the vulnerability. Devices should communicate only if it is necessary, to reduce privacy exposing during communication. Also, devices must be able to disconnect from the network if it is inactivity to minimize tracking of location information. The authorized device only allowed to communicate and if it is turned on, it must re-authenticate itself to the network before start dealing with any information .

C. Privacy in Storage

To protect information privacy, store only the needed and important information to keep the least possible amount of stored information. Information is transported only in case of "need-to-know". Anonymization could be used to disguise the identity of the stored information. A database must limit access to statistical data only. To ensure independency of the output on other database records, differential privacy can be used or adding noise technique .

D. Privacy at Processing

Personal and sensitive data must be processed in a suitable manner and for the processing aim only. The acceptance and the data owner authentication are necessary gained before exposing personal information to third parties. Digital Rights Management

IV. Discussion

Security and privacy issues has a significant impact on the adaptation of IoT. The growing research in this area should consider the security and privacy requirements at each layer and at each development point and address them. As the number of connected heterogeneous nodes increase rapidly and most of the data in the IoT is sensitive and/or personal data, the challenges facing the complexity of the implementation of security solutions are rising. IoT is easy to attack at each layer which makes tackling the security issues a critical area of research. IoT security main requirements include: confidentiality, authorization, authenticity, integrity, and availability. Security challenges in IoT such as service quality, confidentiality and reliability, confidentiality, managing and securing big data, software and hardware vulnerability and creating relevant standards are still open issues and not fully addressed [9]. Authentication and identification are fundamental for IoT data privacy, which is also a main security issue in IoT. However, it faces many neglect while it must be preserved at each part of IoT. Protecting IoT require appropriate security frameworks that covers all IoT layer-security issues. Further research is needed to develop and design proper security solutions for IoT that considers the limitation of its devices. In addition, there is a need for developing a holistic security and privacy frameworks that tackle the identified issues at each layer and consider influencing factors.

V. Conclusion

This paper provided a short introduction to IoT and its 3-layer architecture, reviewed the major IoT security challenges and requirements, highlighted some proposed solutions for security in IoT and discussed the privacy challenges in the IoT. Security and privacy challenges can affect the growth of usage of IoT. There is a need for developing holistic security and privacy frameworks that considers the challenges in IoT environment and relevant influencing factors. Also, proposed security solutions should consider the limitations of IoT devices resources.

Sources:

ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8993036&tag=1

mdpi.com/1424-8220/20/13/3625

softcomputing.net/hamoud2016b.pdf