International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Survey on Security and Privacy under Internet of Things

Jambunathan.S[1], Niranjan.R[2], Gowtham.K[3]
[1]Assistant Professor, Dept. of CS., SKASC
[2, 3]Student, II B.Sc. Computer Science, SKASC

***Abstract*— *IoT-Internet of Things is a modern technology which is gaining rapidly and popularly, not only in industries and commercial purpose, it also important in personal life by means of the devices called as smart devices which are used at home. The Internet of Things gives the new business opportunities, companies and firms are trying to understand the concepts of IoT revolution on their purpose. Radio Frequency Identification (RFID) is helping organizations to to construct an automated and interconnected smartest environment by tracking and identifying the object, motivating the first step towards an IoT-enabled world. Securing the Internet of Things gives us the network and cyber security research with knowledge they need to know regarding security in the Internet of Things. This chapter summarizes recent research results in the area of IoT security. It emphasizes the challenges of privacy and security in Iot. The discussion considers. A four layer security architecture is described, consisting of the sensing layer, network layer, service layer, and application-interface layer.*

Keywords*— *Internet of Things (IoT); cybersecurty; Radio Frequency Identification; data security; privacy; sensing layer; network layer; service layer;network layer; service layer; application-interfce layer.

I. INTRODUCTION

In Iot, the privacy and security requirements are more important than anything else. There cannot be any other compromises in the Iot ecosystem to enlarge the benefits of mankind. A small loop hole is sufficient to cause difficulties to large organizations, governments, and individual citizens. Due to advances in Iot technology, every single object can affectively attached to a sensor. As a result, the amount of data collected by the Iot technologies is expanding at a higher rate as more number of sensors are added to the network. Nowadays, there are a large number of network points to Wireless Sensor Networks (WSN) and these to develop at a steady rate. The larger the number of entry points and sensors, the higher the level of vulnerability and risk of security breaches. Thus many Iot consumers have become concerned about security and protection of their privacy. This is somewhat expected given the fact that one function of Iot is to store and share private data. The main challenges and disadvantage users may encounter in the adoption of Iot is that hey lack full control in their sensitive data.

To address the security challenges in Iot, we will analyze the security problems in Iot based on four layer architecture.

II. PRIVACY

A. What is Privacy?

The term “privacy” is one of the important terms in today’s technological society, and its definition has spreaded significantly in recent times. People may have different thoughts on what privacy is and represents; as such, it is worthwhile presenting an overview of the concept of privacy before examining before examining specific branches of privacy concerns that are attributable to the systems provided by the IoT. The word privacy is very much an important term that means different things to different people. In general, privacy is the right or ability of an individual to determine what, when, and how his or her personal information should be disclosed to others. In terms of the IoT, privacy directly relates to the ability of IoT systems to keep the data that is transmitted between objects secure from non-authorized users.

Many critics claim that privacy is dead, since our personal information is already stored in various locations over which we have no control and that we cannot control our privacy if we do not know who is accessing our data. It does not matter how careful we are with our personal data, by subscribing to IoT services, we relinquish some control over our personal information. No doubt, IoT users would be more content if they could access and benefit from IoT functionality and services safe in the knowledge that their personal information and security was fully safeguarded. However, the distance between the user and the physical location of the data creates barriers to this. To overcome these issues, it is necessary to ensure a root of trust at the hardware level.

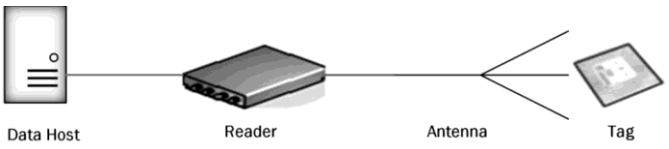
B. Radio Frequency Identification (RFID)

Radio frequency identification (RFID) forms the backbone of IoT. Originally proposed for the military in the 1940s, RFID is by no means a new product. It allows physical objects to be identified and differentiated from other objects and provides the functionality for things to be visually tracked. RFID exists in a wide range of environments and is expected to permeate more areas of our lives in the future. It has been used in many different areas including security control, toll collection control, packaging, supply chain, and distribution. When used responsibly, RFID can benefit people in many different ways; in fact, it can even save lives. However, RFID also introduces critical personal privacy and security challenges since the data stored and transmitted by RFID can be easily hacked. This entails that individuals who carry an RFID tag are at risk of privacy violations.

An RFID consists of three main components: the tag (transponder), the reader (antenna), and the host computer (database/data processor). The RFID tag contains a small microchip and a transmitter that can only be activated by an RFID reader, to which the tag returns its signal. The

Jambunathan.S, Niranjan.R, and Gowtham.K, “Survey on security and privacy under internet of things,” *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 1, pp. 53-58, 2018.

information shared between the tag and the reader is usually protected by network protocols. The components of a typical RFID system are illustrated in the below diagram.



The tag works as a unique identifier of the item it is linked with. The reader communicates with the RFID tag to obtain and identify the information that is stored in the tag. The host computer is responsible for processing the information collected from the RFID tags by associating each tag with its arbitrary records. RFIDs have evolved into a variety of forms and applications, both active and passive. In the active RFIDs, a tag has its own transmitter along with the power source, whereas, in passive RFIDs, the tag is activated by a radio signal from the reader's antenna.

C. Privacy Requirements for the IoT.

Some IoT applications are tightly linked to sensitive infrastructures and strategic services such as the distribution of water and electricity. Other applications handle sensitive information about people, such as their location and movements, or their health and purchasing preferences. Confidence in IoT will depend on the protection it provides to people's privacy and the levels of security it guarantees to systems and processes.

Data privacy

Data privacy complements confidential data transmission in the sense that a stored data record must not expose undesired properties, such as the identity of a person. This requirement is an enormous challenge in the IoT, as so many sensing devices collect personal information. Large amount of such data becomes PII when combined together.

Anonymity

Achieving anonymity is a tough challenge as wearable and mobile devices may leak PII such as IP addresses and location unknowingly. Technologies such as anonymous credentials and onion routing exist, but may not scale well with the IoT.

Pseudonymity

Pseudonymity trades off anonymity with accountability. With pseudonymity, actions of a person are linked with a pseudonym, a random identifier, rather than an identity. While pseudonyms may resolve privacy and accountability concerns in the IoT, standardized solutions that accompany multiple domains are required.

Unlinkability

Unlinkability qualifies pseudonymity in the sense that specific actions of the same person must not be linked together. Unlinkability protects from profiling in the IoT. While pseudonyms may solve unlinkability, i.e., a different pseudonym is used for every action, cross-implications with anonymity, in particular unknown meta-data, remain a challenge. Furthermore, some entity can always link every pseudonym to a person, and can thus also link all actions of that person.

The IoT finds application in many fields, such as health-care, home automation, smart cities, and environmental monitoring. All the IoT applications must protect user's movements, habits, interactions and private life.

D. IoT Privacy Challenges

As medical and well-being devices are increasingly being adopted by users and personalized medicine and health care applications are being designed and deployed that rely on continuous fine-grained data acquisition from these devices, the human body is becoming a rich source of information. Such information is typically collected from devices and then uploaded to some cloud and/or transmitted to other devices, such as mobile phones, which in turn may forward the information to other parties. The collected information is typically very rich and often includes meta-data such as location, time, and context, thus making possible to easily infer personal habits, behaviors, and preferences of individuals. It is thus clear that on one side such information has to be carefully protected by all parties involved in its acquisition, management, and use, but also users should be provided with suitable, easy to use tools to protect their privacy and support anonymity depending on specific context. The privacy and data protection challenges related to IoT are:

1. *Lack of control and information asymmetry:* interaction between objects that communicate automatically and by default, between objects and individual devices, between individuals and other objects, and between objects and back-end systems, which will result in the generation of data flows that can hardly be managed with the traditional tools used to ensure the adequate protection of the data subject's interests and rights.
2. *Quality of the user´s consent:* the possibility of rejecting certain services is not a real alternative in IoT and classic mechanisms used to obtain consent may be difficult to apply. Therefore, new ways of obtaining the user´s valid consent should be considered, including implementing consent mechanisms through the devices themselves as privacy proxies.
3. *Inferences derived from data and repurposing of original processing:* The IoT stakeholders will make sure the raw information is used for purposes that are compatible with original purposes which the users know already.
4. *Intrusive identification of behaviour patterns and profiling:* Proliferation of sensors is used to generate knowledge even from anonymous data source which in turn helps to get the detailed behavior patterns.
5. *Limitations on the possibility of remaining anonymous when using services*; and
6. *Security risks* - weak points can occur not only at device level but also in the communication links, storage infrastructure and other inputs of this ecosystem.

E. Privacy Threats

Although the innovation potential of IoT technology is large, this technology also has numerous inherent

Jambunathan.S, Niranjan.R, and Gowtham.K, "Survey on security and privacy under internet of things," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 1, pp. 53-58, 2018.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

vulnerabilities. RFID intensify the privacy issue of IoT because they make information readily available and accessible through a wireless network. Some of the more common privacy threats that are associated with the IoT are as follows:

• *Location Tracking Threats:* One may wonder about the consequences of a world full of tagged objects. Given the ability to associate an RFID tag with a person, her or his location can be detected and tracked. This threat entails that a person's identity can be readily associated with an object. A hidden RFID reader can possibly be installed at any specific location for the purposes of tracking someone. An individual who carries a tag can be easily tracked, and that eventually leads to user privacy violation. Unfortunately, an RFID tag transmits data responds and responds to a given signal without alerting its bearer or owner. As a consequence, an individual can be tracked without his or her knowledge.

• *Information Leakage:* This threat correlates directly with the disclosure of the information that an RFID system has collected. The leakage of information may occur when the key pieces of personal information associated with a product or item are disclosed. This information may include important data, such as full name, address, social security, health history, and financial accounts. For example, pharmaceutical products that are tagged may store information about a person's health history. RFID tags are not designed to store large amounts of data. However, the data that is stored on the tag can potentially be used to access the large quantities of data that are stored on the database host.

III. Security

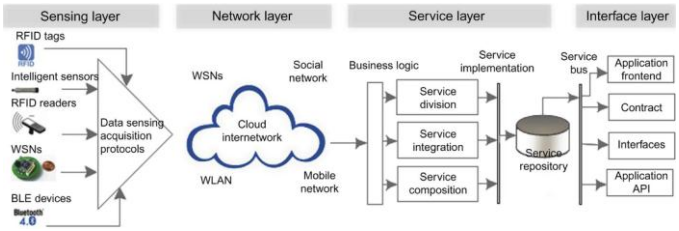
A. Security Requirements in IoT Architecture

A critical requirement of IoT is that the devices must be interconnected, which makes it be able to perform specific tasks, such as sensing, communicating, information processing, etc. The IoT is able to acquire, transmit, and process the information from the IoT end-nodes (such as RFID devices, sensors, gateway, intelligent devices, etc.) via network to accomplish highly complex tasks. The IoT should be able to provide applications with strong security protection (e.g., for online payment application, the IoT should be able to protect the integrity of payment information).

The system architecture must provide operational guarantees for the IoT, which bridges the gap between the physical devices and the virtual worlds. In designing the framework of IoT, following factors should be taken into consideration: (1) technical factors, such as sensing techniques, communication methods, network technologies, etc.; (2) security protection, such as information confidentiality, transmission security, privacy protection, etc.; (3) business issues, such as business models, business processes, etc. Currently, the SoA has been successfully applied to IoT design, where the applications are moving towards service-oriented integration technologies. In business domain, the complex applications among diverse services have been appearing. Services reside in different layers of the IoT such as: sensing layer, network layer, services layer, and application–interface layer. The services-based application will heavily depend on the architecture of IoT, which consists of four layers

- Sensing layer is integrated with end components of IoT to sense and acquire the information of devices;
- Network layer is the infrastructure to support wireless or wired connections among things;
- Service layer is to provide and manage services required by users or applications;
- Application–interfaces layer consists of interaction methods with users or applications.

The security requirements on each layer might be different due to its features. In general, the security solution for the IoT considers following requirements: (1) sensing layer and IoT end-node security requirements, (2) network layer security requirements, (3) service layer security requirements, (4) application–interface layer security requirements, (5) the security requirements between layers, and (6) security requirements for services running and maintenance.



B. Sensing Layer

The IoT is a multilayer network that interconnects devices for information acquisition, exchange, and processing. At the sensing layer, the intelligent tags and sensor networks are able to automatically sense the environment and exchange data among devices (Li et al., 2014c). In determining the sensing layer of an IoT, the main concerns are:

- Cost, size, resource, and energy consumption. The things might be equipped with sensing devices such as RFID tags, sensors, actuator, etc., which should be designed to minimize required resources as well as cost.
- Deployment. The IoT end-nodes (such as RFID reader, tags, sensors, etc.) can be deployed one-time, or in incremental or random ways depending on application requirements.
- Heterogeneity. A variety of things or hybrid networks make the IoT very heterogeneous.
- Communication. The IoT end-nodes should be designed in such a way that it is able to communicate with each other.
- Networks. The IoT involves hybrid networks, such as Wireless Sensor Networks (WSNs), WMNs, and supervisory control and data acquisition (SCADA) systems.

The security is an important concern in sensing layer. It is expected that IoT could be connected with industrial networks to provide users with smart services. However, it may cause new concerns in devices controlling, such as who can input authentication credentials or decide whether an application should be trusted. The security model in IoT must be able to

Jambunathan.S, Niranjan.R, and Gowtham.K, "Survey on security and privacy under internet of things," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 1, pp. 53-58, 2018.

make its own judgments and decision about whether to accept a command or execute a task. At sensing layer, the devices are designed for low power consumption with constraints resources, which often have limited connectivity. The endless variety of IoT applications poses an equally wide variety of security challenges.

- Devices authentication
- Trusted devices
- Leveraging the security controls and availability of infrastructures in sensing layer.
- In terms of software update, how the sensing devices receive software updates or security patches in a timely manner without impairing functional safety or incurring significant recertification costs every time a patch is rolled out.

In this layer, the security concerns can be classified into two main categories:

- The security requirements at IoT end-node: physically security protection, access control, authentication, nonrepudiation, confidentiality, integrity, availability, and privacy.
- The security requirements in sensing layer: confidentiality, data source authentication, device authentication, integrity, availability, and timeless.

Security Threats	Description
Unauthorized access	Due to physically capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker
Availability	The end-node stops to work since physically captured or attacked logically
Spoofing attack	With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data
Selfish Threat	Some IoT end-nodes stop working to save resources or bandwith to cause the failure of network
Malicious code	Virus, Trojan and junk message that can cause software failure
DoS	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on routing path

To secure devices in this layer before users are at risk, following actions should be taken:

- Implement security standards for IoT and ensure all devices are produced by meeting specific security standards
- Build trust worthy data sensing system and review the security of all devices/components
- Forensically identify and trace the source of users
- Software or firmware at IoT end-node should be securely designed.

C. Network layer

The network layer connects all things in IoT and allows them to be aware of their surroundings. It is capable of aggregating data from existing IT infrastructures and then transmitted to other layers, such as sensing layer, service layers, etc. The IoT connects a variety of different networks, which may cause a lot of difficulties on network problems, security problems, and communication problems.

The deployment, management, and scheduling of networks are essential for the network layer in IoT. This enables devices to perform tasks collaboratively. In the networking layer, the following issues should be addressed:

- Network management technologies including the management for fixed, wireless, mobile networks,
- Network energy efficiency,
- Requirements of QoS,
- Technologies for mining and searching,
- Information confidentiality,
- Security and privacy.

Among these issues, information confidentiality and human privacy and security are critical because of its deployment, mobility, and complexity. The existing network security technologies can provide a basis for privacy and security protection in IoT, but more works still need to be done. The security requirements in network layer involve:

- Overall security requirements, including confidentiality, integrity, privacy protection, authentication, group authentication, keys protection, availability, etc.
- Privacy leakage: Since some IoT devices physically located in untrusted places, which cause potential risks for attackers to physically find the privacy information such as user identification, etc.
- Communication security: It involves the integrity and confidentiality of signaling in IoT communications.
- Over connected: The over connected IoT may run risk of losing control of the user. Two security concerns may be caused: (1) DoS attack, the bandwidth required by signaling authentication can cause network congestion and further cause DoS; (2) Keys security, for the over connected network, the keys operations could cause heavy network resources consumption.
- MITM attack: The attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the attacker controls the entire conversation.
- Fake network message: Attackers could create fake signaling to isolate/misoperate the devices from the IoT.

Security Threats	Description
Data breach	Information released of secure information to an untrusted environment
Public key and private key	It comprimises of keys in networks
Malicious code	Virus, Trojan and junk message that can cause software failure
DoS	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on routing path

Jambunathan.S, Niranjan.R, and Gowtham.K, "Survey on security and privacy under internet of things," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 1, pp. 53-58, 2018.

The network infrastructure and protocols developed for IoT are different with existing IP network, special efforts are needed on following security concern:

- Authentication/Authorization, which involves vulnerabilities such as password, access control, etc.
- Secure transport encryption-it is crucial to encrypt the transmission in this layer

D. Service layer

In IoT, the service layer relies on middleware technology, which is an important enabler of services and applications. The service layer provides IoT a cost-effective platform where the hardware and software platforms could be reused. The IoT illustrates the activities required by the middle service specifications, which are undertaken by various standards developed by the service providers and organizations. The service layer is designed based on the common requirements of applications, application programming interfaces (APIs), and service protocols. The core set of services in this layer might include following components: event processing service, integration services, analytics services, UI services, and security and management services. The activities in service layer, such as information exchange, data processing, ontologies databases, communications between services, are conducted by following components:

- Service discovery. It finds infrastructure that can provide the required service and information in an effective way.
- Service composition. It enables the combination and interaction among the connected things. Discovery exploits the relationships of things to find the desired service, and service composition schedules or recreates more suitable services to obtain the most reliable ones.
- Trustworthiness management. It aims to understand the trusted devices and information provided by other services.
- Service APIs. It provides the interactions between services required by users.

Recently, a number of service layer solutions have been reported. The SOCRADES integration architecture is proposed that can be used to interact between applications and service layers effectively); things are abstracted as devices to provide services at low levels as network discovery services, metadata exchange services, and asynchronous publish and subscribe event, A representational state transfer is defined to increase interoperability between loosely coupled services and distributed applications. The services layer introduced a service provisioning process that can provide the interaction between applications and services. It is important to design an effective security strategy to protect services against attacks in the service layer. The security requirements in the service layer include:

- Authorization, service authentication, group authentication, privacy protection, integrity, security of keys, nonrepudiation, antireplay, availability, etc.
- Privacy leakage. The main concern in this layer involves privacy leakage and malicious location tracking.
- Service abuses. In IoT the service abuse attack involves: (i) illegal abuse of services; (ii) abuse of unsubscribed services.
- Node identify masquerade.
- DoS attack.
- Replay attack, the attacker resends the data.
- Service information sniffer and manipulation.
- Repudiation in service layer, it includes the communication repudiation and services repudiation.

Security Threats	Description
Privacy threats	Privacy leakage or malicious location tracking
Services abuse	Unauthorized user access services or the authorized users access unsubscribed services
Identity masquerade	The IoT end-device, node, or gateway are masqueraded by attacker
Service information manipulation	The information in services is manipulated by the attacker
Repudiation	Denial of the operations have been done
DoS	An attempt to make an Iot end-node resource unavailable to its users
Reply attack	The attack resends the information to spoof the receiver
Routing attack	Attacks on a routing path

Ensure the data in service layer security is crucial but it is difficult. It involves fragmented, full of competing standards, and proprietary solutions. The SoA is very helpful to improve the security of this layer, but following challenges still need to be faced when building an IoT services or application:

- Data transmission security between service and/or layers;
- Secure services management, such as service identification, access control, services composite, etc.

E. Application Interface Layer

The application–interface layer involves a variety of applications and interfaces from RFID tag tracking to smart home, which are implemented by standard protocols as well as service-composition technologies (Ning et al., 2013). The requirements in application–interface layer strongly depend on the applications. For the application maintenance, following security requirements will be involved:

- Remote safe configuration, software downloading and updating, security patches, administrator authentication, unified security platform, etc.

For the security requirements on communications between layers:

- Integrity and confidentiality for transmission between layers, cross-layer authentication and authorization, sensitive information isolation, etc.

In IoT in designing the security solutions, following rules should be helpful:

a. Since most constrained IoT end-nodes work in an unattended manner, the designer should pay more attention to the safety of these nodes;
b. As Iot involves billions of clustering nodes, the security solutions should be designed based on energy efficiency schemes;
c. The light security scheme at IoT end-nodes might be different with existing network security solutions;

Jambunathan.S, Niranjan.R, and Gowtham.K, "Survey on security and privacy under internet of things," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 1, pp. 53-58, 2018.

however, we should design security solutions in a big enough range for all parts in IoT.

The application-interface layer bridges the IoT system with user applications, which should be able to ensure that the interaction of IoT systems with other applications or users are legal and can be trusted.

Security Threats	Description
Remote configuration	Fail to configure at interfaces
Misconfiguration	Misconfiguration at remote IoT end-node, end-device, or end-gateway
Security management	Log and keys leakage
Management system	Failure of management system

REFERENCES

[1] Li Da Xu and Shancang Li, "Securing the internet of things", *Syngress*, Jan 11 2017.
[2] Marwan Omar, Mohamed Eltayeb, and Maurice Dawson, "Security solutions for hyperconnectivity and the internet of things", *IGI Global*, August 30 2016.
[3] In lee, " The internet of things in the modern buisness environment", *IGI Global*, March 31 2017.
[4] Jojo Moolayil, "Smarter decisions-The intersection of internet of things and decision science", Packt Publishing, July 29 2016.