Internet of Things (IoT) Security - A Survey

Nandini Krupa Krishnamurthy
Clemson University
nandink@clemson.edu

***Abstract*—In the past decade, Internet of Things (IoT) has taken the world by storm. Its increasing popularity is also an interesting topic of research. Security and Privacy are two main challenges of an IoT system. This paper talks about Security in IoT system. It starts with the Introduction and then moves ahead to describe the architecture of an IoT system in detail. Further, it talks about the techniques that are present in IoT. The third section describes some of the interesting attacks on IoTs. The fourth sections elaborates on why is IoT security important and what are the challenges faced. The last section talks about the open research areas in this domain.**

I. Introduction

IoT internet of things is something that the world is attracted to in recent years. IoT has made everyday life easier. IoT is considered to be the internet of the future and is probably going to contain billions of communicating devices, which are intelligent as well as easy to handle. This would probably make the world a smaller place. This is the future of the Internet which heterogeneously connect devices to the internet. IoT gives new capabilities to connected devices. [1] IoT has developed its own importance in probably almost all the fields including the education, industry, and commerce. The number of things in the living space is more than the current world population. Huge research in this area is to make these things communicate like how computer devices communicate with each other with the help of the Internet [2]. Now having said all these, we can think of IoT as a collection of wireless communication technologies which includes sensor networks, mobile networks, and actuators. Each element of IoT is called as a thing and will possess a unique address. These things communicate using Radio-Frequency Identification (RFID) and synchronously work together to achieve a common objective. It is also important to maintain Security in IoT to realistically determine its users, its privileges and also restrictions. By 2025, IoT will connect everything in our life as stated by US National Intelligence [2]. And hence, IoT becomes a topic of interest and also a lot of researches are going on in this field to make IoT affordable and also user-friendly. Before we discuss the security in IoT or the security that IoT provides let us first see the architecture of IoT.

A. IoT Architecture

IoT demands that all the components in it are well connected. IoT architecture must be such that it bridges the physical and virtual components of the IoT system along with guaranteed operations. Therefore, IoT architecture must be carefully designed keeping in mind many factors including networking, communication, business processes, and security [1]. The important characteristics of an IoT architecture must include extensibility, scalability, and interoperability. It must also adapt to dynamic working should also support unambiguous communication.

The basic layered architecture of IoT consists of five layers as shown below in the Figure2.

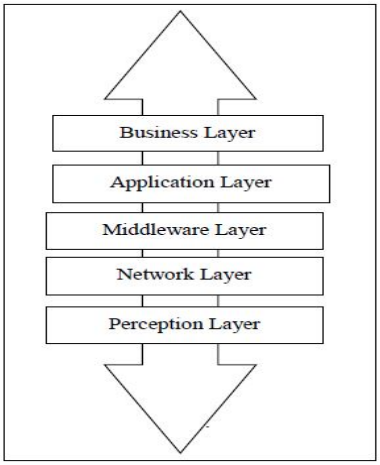

Fig. 1. Basic five layered architecture of IoT [4]

. Though this is the basic structure of a IoT, there is one more architecture called the Service Oriented Architecture of IoT. It is one of the most important architectures developed for IoT.This survey paper mainly deals with Service Oriented Architecture. This architecture as shown in Fig. 1 consists of four layers namely,

1) Sensing Layer
2) Network Layer
3) Service Layer
4) Interfaces Layer

Sensing layer consists of Hardware object that senses the status is of things. Network Layer supports communication among the things of IoT using wireless or wired communication. Service Layer helps in the creation and management of services as required by users and applications. The interactive layer consists of methods of interaction between users and applications. Now let us go through each of the layers in detail.

1) **Sensing Layer:** IoT is a massive network of interconnected components, both physical and virtual, that can be connected remotely. The sensor layer is used by

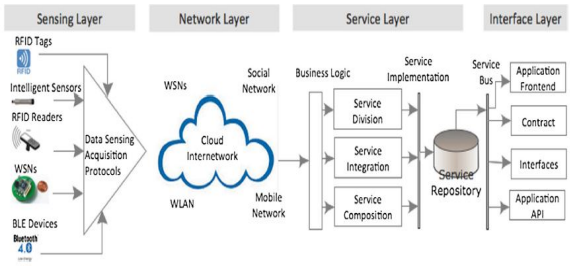

Fig. 2. IoT Service Oriented Architecture [2]

the smart IoT systems to sense the environmental stimuli and also help in exchange of data. RFID used by IoTs in the modern world makes them more versatile easily usable which extensions and increases IoT functionalities. This helps them in identifying the things around them accurately and also monitor the environment for various purposes and applications. Everything in the system or every object in the IoT system holds a unique identifier called the digital identity which helps to track these in the digital domain. This unique identifier is known as universal unique identifier (UUID). Universal unique identifier helps in deploying services in the networks. Identification of the kind of sensing layer required by the IoT devices needs the following aspects to be taken care of [1].

a) Cost, size, resource, and energy consumption
b) Deployment: one-time, or incrementally, or randomly
c) Heterogeneity
d) Communication: accessible and retrievable
e) Network: multi-hop, mesh or ad hoc networks
f) Energy efficiency
g) Protocols: WLAN, ZigBee, and Bluetooth

2) **Network Layer:** Network layer is used to connect things in the IoT and disconnection makes IoT be aware of its surroundings. Network layers also helps in shading the data between two connected components which is the basic need for management and processing in IoT. Additionally it also collects data from the currently available IT infrastructure. send this data can be transferred to higher levels for further processing and services. service-oriented architecture the components of IoT are installed in a heterogeneous Network. Network layers also has to have quality of service guarantee. also it is also always preferred to discovered the components of IoT automatically and map them. mapping in walls scheduling, deploying, and managing the roles of all the things. Some of the issues to be addressed in network layer are network management issues, Network Energy Efficiency, Mining and searching Technologies, security and privacy, and quality of service.
3) **Service layer:** Service layer is built upon middleware technology. This is used to enable services and applications in IoT. this also helps in reusing hardware and software platforms. this layer works on top of network layer the advantage of working in this way is it can directly locate services needed by an application and obtain meta-data on the run. Though there are many varieties of service layer, a practical approach would be to consider minimum set of applications that run on network layer , APIs and also set of protocols supporting all these. the functions of service layer include information exchange and Storage , data management, and engines and communication search. The components of the service layer as listed below carry out all the about set functions.

a) Service Discovery: searches for objects that can provide quality service and sufficient information to carry out necessary activities.
b) Service composition: helps in the interaction between components of an IoT system.
c) Trustworthiness management: this component helps the layer to understand how the information provided by other systems have to be processed.
d) Service APIs: as the name suggests, it provides the interactions between services and users.

4) **Interface layer:** There are a lot of IoTs in the market provided by different vendors and these work with different capabilities and have different standards. To understand how they interact compatibility has to be considered. Compatibility issues arise in information exchange, communication, and event processing. Therefore, there is a strong need enforced Management Systems simplify interconnection of things. This can be done using an interface profile (IFP). An interface profile can be viewed as a subset of service standards that helps with minimum interactions between the applications on the application layer. These are also used to specify the specifications between applications and services. An example of this is the Universal Plug and Play (UPnP).

II. Working of an IoT - Building Blocks and Technologies

The functionality of an IoT can be thoroughly understood by understanding the basic structure or the building blocks of it. To deliver all the functionality there are six blocks of IoT. These are as listed below [5].

1) Identification
2) Sensing
3) Communication
4) Computation
5) Service
6) Semantics

Fig. 3 shows the building blocks and technologies of IoT. Let us know briefly discuss about each of these.

1) Identification: There are huge demands created for IoT. Therefore it is necessary to understand and identify what

IoT Elements		Samples
Identification	Naming	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, , LTE-A
Computation	Hardware	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, Smart Phones
	Software	OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc.)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)
Semantic		RDF, OWL, EXI

Fig. 3. Building Blocks and Technologies of IoT [5]

the demand is created to carry out its services [5]. Many identification methods are available for this purpose. Most famous of them are Electronic Product Codes (EPC) and Ubiquitous Quotes (uCode).Further, the Object ID and address have to be specified. types of IoT objects include ipv4 and IPv6 TV6 typically addresses low power wireless networks. object identification and address have to be distinguished because these identification methods are not unique. Additionally, objects within a network tend to use public IPs another private IP.

2) Sensing: The act of sensing is nothing but sensing the data from related objects in the network and then sending these data back to a data warehouse where these can be processed further.. examples of sensors are smart sensors, actuators or wearable sensing devices [5]. Some of the examples of IoT products are Raspberry Pi and BeagleBone Black. Single board computers along with sensors, TCP/IP functions, and security services are used to make IoT products work.

3) Communication: Communication is crucial inIoT devices because they connect various heterogeneous devices in a network. All of these at together to perform a specific service. There are various communication protocols used by IoT devices. Some of these are WiFi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-Advanced. Some examples of specific communication technologies are RFID, Near Field Communication (NFC) and ultra-wide bandwidth (UWB). The RFID is a simple chip and is attached to an object. it is used for transmitting why to use a signal to a tag and receive replies from it. this, in turn, is sent to the database. RFID tags candy active, passive or semi-active. NFC protocol works at a high-frequency band. The UWB supports communication for a low coverage area. This uses low energy and high bandwidth. One of the most communication Technologies is Wi-Fi. This uses radio waves and exchanges the data among the things within a range of hundred meters. this is special because it doesn't need a router for the exchange of data and communication between devices. Bluetooth is another communication technology that uses low energy and high speed to support connectivity in IoT.

4) Computation: Computation in IoT is carried out by a combination of both hardware and software. The hardware consists of processing units such as microcontrollers, microprocessors, SOCs and FPGAs. Software applications are called to the brain of an IoT. Hardware platforms currently available are Arduino, UDOO, FriendlyARM, Intel Galileo, Raspberry PI, Gadgeteer, BeagleBone, Cubieboard, Z1, WiSense, Mulle, and T-Mote Sky [5]. Many software platforms are provided by IoT. Among them, the main important one is the operating system. there are real-time operating systems (RTOS) which are used for development of RTOS based IoT. TinyOS, LiteOS, and Riot OS are known for their lightweight OS that is specifically designed for IoT environments. Google's Open Auto Alliance(OAA) plans to build new features to establish IoT on Android. Another important computational part is the cloud. These are based on the services that the cloud offers. in a nutshell, they allow smart sensors to send data to the cloud, process them in real time and send the data back to the end users. There are a lot of three platforms are available on the cloud to serve all these functionalities.

5) Service: The services offered by IoT can be classified under for classes. they are Identity Related Services, Information Aggregation Services, Collaborative Aware Services, and Ubiquitous Services. Identity-Related Services are the most basic and also the most important Services as these are also used in another type of services. Information Aggression Services think about the collection of data and provide these as raw data for the IoT to process. Collaborative-Aware Services are built on top of Information Aggregation Services. These help in decision-making and reaction to these decisions. Ubiquitous Services act as subsidiary services and their main objective is to provide Collaborative Services to anyone who needs them and at whatever time they need them.

6) Semantics: Semantics is the ability of an IoT to extract the required knowledge from a different type of devices to carry on the required process. This is known as knowledge extraction. It includes recognizing and analyzing the data so as to make correct decisions at the correct time with correct data. Therefore semantically presents the brain of an IoT device as meet the demands of the specific user by sending them the appropriate content as required by them. This activity is supported by various Semantic Web Technologies including Resource Description Framework (RDF) and the Web Ontology Language (OWL).

III. Attacks on IoT Security

Since this paper talks about IoT security, let us underfstand some of the basic security attacks on IoTs. These can be broadly divided into four groups as explained below [6].

A. Physical Attacks

These attacks focus on hardware components of an IoT device [6].

1) **Node Tempering:** In this form of attack, the attacker changes the working of the prey node and can obtain the sensitive information from this hampered node such as encryption data.
2) **RF Interference on RFIDs:** A special type of attack where DoS type of attack is performed by the attacker using end voice signals over radio frequency signals which in turn are used by RFID for communication.
3) **Node Jamming in WSNs:** The wireless communication can be hampered by the usage of jammers, causing DoS attacks.
4) **Malicious Node Injection:** In this type of attack, the attacker physically injects malicious matter between two nodes . This might also extend to more than two nodes. By this, nodes modify the data and pass on incorrect data. The attacker, no in turn, uses multiple nodes for the same purpose to create an attack.
5) **Physical Damage:** This, as the term says, causing physical damage to the components of an IoT. This leads to a Denial of Service attack.
6) **Social Engineering :** The main goal of an attacker here is to obtain sensitive information and physical talk to users of an IoT and manipulate them.
7) **Sleep Deprivation Attack:** Here, nodes are shut down to due to excessive use of power by the attacker..

B. Network Attacks

These types of attacks are focussed on network of the system [6].

1) **Traffic Analysis attack:** Here the attackers interrupts the messaging passing process and examines it to obtain network information.
2) **RFID Spoofing:** Here, an attacker spoofs RFID signals. Then he accesses the information from RFID signals. The systems treat these spoofed signals as RFID and accepts it.
3) **RFID Cloning:** In this type of attack, an attacker copies an already existing RFID tag to another RFID tag. When this happens, the attacker can insert malicious data or able to control the passage of data.
4) **RFID Unauthorized Access:** If the RFID system doesn't provide correct authentication that attackers can absorb information, alter or even remove them.
5) **Sinkhole attack:** In this form of attack an attacker uses a node inside a network for his benefit. This is called as compromising the node. This compromised node then sends fake information to its neighbors saying that it has the shortest path to the base station. By doing this it attracts the traffic . Now, it can alter the information in the packet or can also drop it.
6) **Man in the Middle Attacks:** The information between two nodes is obtained by eavesdropping. This is called as Man in Middle Attack.
7) **Denial of Service:** When an attacker floods the network with traffic thus denying the resource for processing information. This stops the service from its intended users.
8) **Routing Information Attacks:** Here, the attacker makes the network inefficient by spoofing, modifying or sensing incorrect routing information thus resulting in dropping of the packets or forwarding wrong information.
9) **Sybil Attack:** In this form of attack, a node takes copies the identities of multiple nodes and fakes their identity.

C. Software Attacks

When an attack is performed by using virus, worm, spyware, adware etc. to steal data and/or to deny the services, it qualifies to be a Software Attack [6].

1) **Phishing Attacks:** : Attack on the private information of the user is called as phishing attack.
2) **Virus, Worms, Trojan horse, Spyware and Aware:** : When malicious codes as these are injected in to the system, an attack happens. These can be spread through attachments in mails or even downloading files from internet.
3) **Malicious Scripts:** By injection of malicious script into the system, an attacker can gain control of it.
4) **Denial of Service:** When an attacker floods the network with traffic thus denying the resource for processing information. This stops the service from its intended users.

D. Encryption Attacks

These types of attacks use methods to destroy encryption and obtain the private key [6].

1) **Side-channel Attacks:** The side channel emitted by the encrypted node can be used by the attacker for his benefits. It contains information on power, faults, frequency etc., which may be used by the attacker to obtain the encryption key.
2) **Cryptanlysis attack:** Here, the attacker uses plaintext or ciphertext to obtain the encryption key. Type of attacks are based on what methods is used. The methods are:
   - Ciphertext Only Attack
   - Known Plaintext Attack
   - Chosen Plaintext Attack
   - Chosen Ciphertext Attack
3) **Man in the Middle Attacks:** When two nodes are exchanging the key, the attackers comes in between and steals the key.

IV. Challenges to IoT Security

Though IoT has provided technologies for everyday uses, they have their own challenges to be faced escpicially on security grounds. Some of them are listed below [9]

1) Botnets: When a hacker wants to use a remotely working machine connected by internet for illegal activities, he makes use of a botnet. These activities also include the usage of an Enterprise's devices as botnets without the knowledge of the rightful owners. Thus,there is a need to develop software which can detect and combat the illegal activities of a botnet.
2) The ever increasing number of IoTs: The number of IoTs are said to reach 20 billion 2020, meaning an increase in security breach and risks of security.
3) Lack of encryption: IoTs lack storage and processing capabilities as that of a traditional computer. This encourages the hackers to manipulate algorithms in IoTs and use them for their own benefit.
4) Weak default passwords: There are, even now, a large number of IoTs in both enterprises and also households that use the password the IoT came along with. These passwords are never changed. These default passwords would be easy to guess and thus becomes vulnerable to attacks.
5) Infrequent patching: IoTs are not updated for the recent software updates periodically. Older the software, more is the risk of security breach.
6) User privacy risk: When an IoT is attacked, there is a huge risk of user-data being compromised. This is one of the top IoT security challenges.
7) Phishing attack: Though a phishing attack is one of the common type of attacks on an IoT, there are no prevalent methods for IoT defense to combat them.

V. Future Trends

The main challenges faced in IoT are its heterogeneity and large scale of objects. This section gives a brief description about the same [7].

A. Object Identification

Object identification is done to ensure the Integrity of the records used in the naming architecture. DNS is still considered to be insecure naming system. Various attacks may happen over the DNS - DNS cache poisoning attack, and man-in-the-middle attack to name a few. Therefore without Integrity protection the naming architecture is insecure. DNSSEC - Domain Name Service Security Extension is the extension for security of DNS . Though DNSSEC seems to be a good option for security, it is still a challenge to deploy in IoT. It has high computation and communication overhead making it no so suitable for IoT.

B. Authentication and Authorization

Public key cryptogram lacks the ability to deploy many schemes due to lack of a global root certificate authority also known as global root CA. As this is absent, it is very tuff to comfortably build a proper authentication unit for IoT. Owing to its heterogeneity and large number, it is not recommended to issue a certificate to an object in IoT. Hence the next challenge is to make authentication and authorization feasible for IoT.

C. Privacy

The biggest challenge is implementing security in an IoT system. These challenges can be broadly classifies into two categories - data collection policy and data anonymization. Data collection refers to the policies using which data collection is done, in other words it refers to the types of data collected and describes about access control of data. This makes the type and the amount of data collected to be restricted. Privacy preservation is also important as this collected data is important. Coming to the next challenge data anonymization. There are two methods here which are important - cryptographic protection and concealment of data relations [7]. Different schemes in cryptographic protection can be adopted to safeguard the data. Concealment of data talks about removal of direct relations between the data and the owner.

D. Lightweight Cryptosystems and Security Protocols

Who two systems are compared - symmetric-key cryptosystems and public-key cryptosystems, public-key cryptosystems provide better security features but suffers significant computational overhead. But, these are needed when high level data integrity and authenticity are needed. So therefore, the next challenge is to devise a method to understand to implement light weight cryptosystems which are both lightweight and provide security features along with low overhead costs.

E. Malware in IoT

Since IoT devices have limited resources, malware thread is a major aspect. High overhead costs may be incurred if antivirus scans for malware on the run. The malware would be crafted into downloader and body. There are also a wide variety of hardware architectures. Considering all these, it is very important to devise a general abstraction of IoT malware.

F. Security Issues from Android

These security issues are particularly important when various devices are connected to android leading to the formation of personal area network (PAN). The main challenge here is sensitive data leakage. Another problem arises when IoT meets Android because Android is opensource thus enhancing the vulnerabilities.

References

[1] Li, Shancang & Da Xu, Li & Zhao, Shanshan. (2014). The internet of things: A survey. Information Systems Frontiers. 17. 10.1007/s10796-014-9492-7.

[2] Saeed, Omsalama. Towards Internet of Things : Survey and Future Vision. (2013).

[3] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.doi: 10.1109/JIOT.2017.2694844

[4] P. Datta and B. Sharma, "A survey on IoT architectures, protocols, security and smart city based applications," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, 2017, pp. 1-5. doi: 10.1109/ICCCNT.2017.8203943

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015. doi: 10.1109/COMST.2015.2444095

[6] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32-37. doi: 10.1109/I-SMAC.2017.8058363

[7] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, 2014, pp. 230-234.doi: 10.1109/SOCA.2014.58

[8] J. Granjal, E. Monteiro and J. S Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, thirdquarter 2015. doi: 10.1109/COMST.2015.2388550

[9] See: https://www.enterprisedigi.com/iot/articles/iot-security-challenges

[10] sayed ali ahmed, Elmustafa & Mohammed, Zeinab. (2017). Internet of Things Applications, Challenges and Related Future Technologies. world scientific news.