IoT Security - A Survey

Shivam Pandit
Clemson University
pandit@clemson.edu

***Abstract*—This Paper presents a survey on Internet of Things (IoT) Security. Being a major research topic for over a decade now, it has raised multiple issues towards the protection of devices connected in the network. Since, it is constantly developing with growing number of devices adding on the IoT platform everyday which raises concerns of ensuring privacy and confidentiality. The future of IoT lies more in secure implementation due to the nature of communication between heterogeneous devices in the network. Typical IoT realization consists of three layers namely Perception, Network and Application layers. Securing these layers is of paramount importance and many researchers have proposed several methods for the same. This paper will present introduction, main techniques, issues and problems and future trends for securing the IoT.**

I. Introduction

Internet of Things (IOT) is a system of interconnected devices that have common goal which was first proposed by Kevin Ashton [1] in 1999. IOT is collection of many interconnected objects, services and devices that communicate with each other and have a common goal. It is a major technological revolution that laid foundation for the realization of smart devices. All existing devices like televisions, cars, refrigerators are turning smart that can communicate with each other and even automate actions without user intervention. All devices in IoT have separate identity to be identified in collection of heterogeneous devices. There are regions in IoT which are identified by IP address but all devices in that region have separate identity.

IoT applications have seen recent new inventions like Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN). RFID enables us to tag each device that can uniquely identify object in the network and WSN enabled all the devices in the network to become a wireless object that can communicate with other objects. IoT has numerous applications that are not only specific to one field but extends to multiple fields like personal and social domain, transportation domain, industry and enterprises and even in services and utility monitoring.

Around 25 billion devices are expected to be part of global network by 2020 that further emphasizes the need of securing it so that there are no privacy and security threats [2]. The nature of the communication between devices which are not only just human to device but can be device to device raises concerns of security since hackers can use one vulnerable device to control the network. It is in developing mode only and without addressing all the security implications we cant expect any future for IoT. No matter how much secure we think the network is, it still has many vulnerabilities which highlights the need of regular patch updates for the objects in IoT. The whole purpose of IoT is to reduce our efforts through smart devices that will perform daily tasks and chores. But since all of the activities are related to the user, security should be number one priority since there are autonomous cars, smart homes, smart banking applications all of which are very safety critical and any unexpected operation can cause economic loss or even threat to human life.

A. IoT Architecture

Typical IoT architecture consists of three layers namely perception, network and application layer [3]. Each layer has specific set of functions and devices. Fig.1 shows a basic three layer architecture of IoT and devices at each layer.

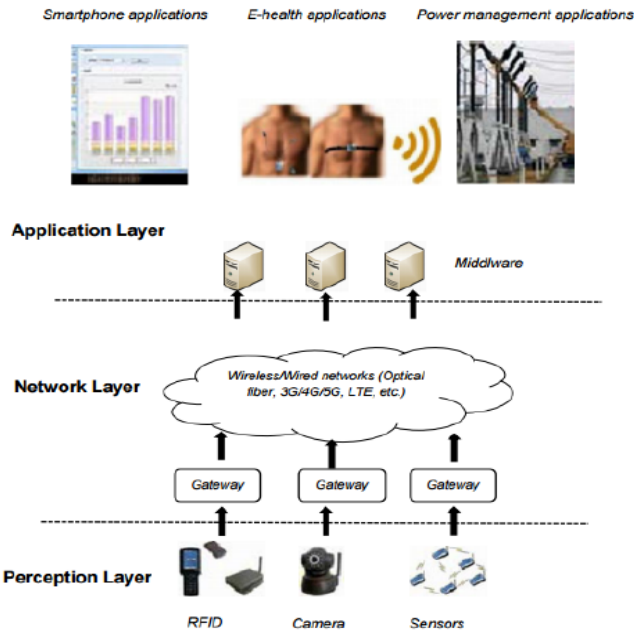

Fig. 1. Three layer IoT architecture Source: researchgate.net

1) **Perception Layer:** This layer consists of sensors and often called as Sensors layer in IoT. The purpose of this layer is to collect data from the environment through sensors and actuators like RFID, barcodes or similar sensor devices. This layer first collects information through sensors and transmits it to the network layer.
2) **Network Layer:** This layer is responsible for data routing and transmission. It gathers information from

perception layer and routes it to relevant processing system through IoT hubs and devices over the internet. Some of the very recent technologies like WiFi, LTE, 3G, etc are used in this layer. So, this layer acts a mediator between different nodes.

3) **Application Layer:** This layer is topmost layer and realizes practical applications of IoT which guarantees authenticity, confidentiality and integrity of the data. Here, we achieve the purpose of IoT implementation.

II. Main Techniques

To secure the IoT, each of the three layers must be secured. Many researchers have worked on many well-defined security architectures which can ensure confidentiality and privacy. We will be discussing the state-of-art techniques that solves security problems in IoT but before that will see how IoT differs from conventional networks [4].

A. IOT security vs Conventional security

There are differences between IoT and conventional networks in terms of security and privacy as shown in Fig 2 below. Conventional security has mostly dynamic topologies whereas IoT devices are setup on LLNs. The IoT nodes have low processing power and are strained in dynamism and memory. Sensor nodes have very less computational power in IoT networks. All methods used are lightweight to ensure nodes are not strained. Conventional networks dont have this issue as they have different implementation and different protocols like wireless fidelity is used in physical layer in conventional networks whereas IoT networks use low power wireless personal area network. In summary, conventional architectures are designed keeping in view user interaction whereas IoT are designed keeping in view device to device communication.

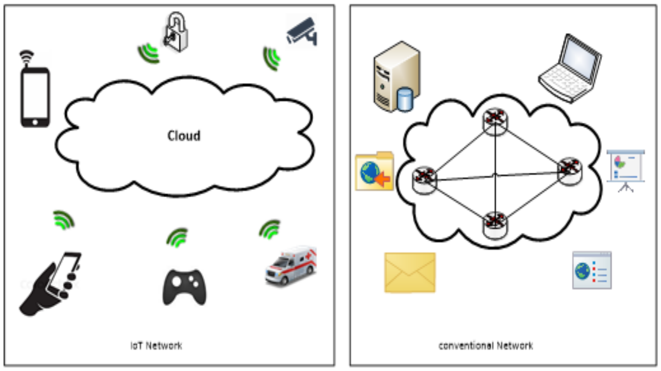

Fig. 2. IoT Network vs. Conventional Network

B. Securing Perception Layer

This is the bottom layer of IoT architecture which is responsible for data gathering while providing various security features. Now, we will be discussing some security aspects associated with this layer which are Authentication, Data Privacy and Privacy of sensitive information.

- **Authentication:** Cryptographic Hash algorithms are used that serves the purpose of authentication through digital signatures. It protects from most attacks including brute force and side-channel attacks.
- **Privacy of Data:**Encryption algorithms like symmetric and asymmetric encryption algorithms such as RSA, DES, etc are used to prevent unauthorized access of the sensor data ensuring security.
- **Privacy of sensitive information:** K-anonymity approach ensures protection of information that are important to user like private information or location data.

C. Securing Network Layer

This layer can be either wireless or wired and is most vulnerable to attacks due to its openness. It can be easily monitored by hackers and vulnerable to eavesdropping, man-in-the-middle attacks. So, security at this layer is very important. This layer has three security purposes that must be addressed.

- **Authentication:** Proper encryption techniques eliminates any unauthorized access to the sensors and address the issue of Authentication. Most common is DoS attack which can impact other networks by generating false traffic and make many devices in the network non-operational.
- **Secure Routing:** We must ensure information packets are securely routed in the network to the destination node. This is very critical since packets can be captured in the middle by the hackers or just sniffed without the knowledge of the receiver node. One safe routing was proposed by researchers called Source Routing that sends the packets to processing system that checks if it was analyzed by intermediate nodes.
- **Privacy of Data:** Since packets can reach the receiver sniffed or partially lost. So, there must be ways to check the integrity of the packets and detect any kinds of intrusion. It should be checked at the receiver side if the packet received is same as that was send from the sender.

D. Securing Application Layer

This is the topmost layer that realizes the IOT application. It also has similar purposes as below layers but different ways for implantation as explained below.

- **Authentication:** To prevent any miscreant from accessing the application, authentication process is used which is like other layers except that it performs authentication within cooperating services too that ensure which processes can communicate with each other. Most popular technique to secure the system is through using virtualization which can prevent many attacks but still is vulnerable to DoS thus keeping scope for lot of research.
- **Intrusion Detection:** This is very important due to attacks getting more sophisticated. Some attacks are so difficult to detect that attackers takes the information and receiver cannot even know if any sniffing happened.

Intrusion detection systems raises alarm when they find any sort of intrusion in the network and can even keep log of the intruder activities. Most popular techniques to achieve intrusion detection system is through data science or anomaly detection approach.

- **Securing Data:** Encryption algorithms along with firewalls and up to date spyware/adware ensures data is secure during transmission from miscreant users.

Apart from securing each IoT layer, there is also a need of security awareness among the end users. Human users on the IoT network must be aware of their roles for safely using IoT without performing any action that can affect some device in the IoT framework which could cascade to other devices in the network due to device to device communication. Secondly, no factory default passwords should be kept on the devices as they are most vulnerable to attacks. Hackers just need a device to control the network due to nature of communication in the IoT framework. Thus, little caution from e

Trust establishment is also important since IoT devices can be administered by multiple users and even change owners. So, there must be smooth transition of access control and permissions. This can be implemented through access-control framework through two mechanisms: token and creation key. All new devices that are added to the IoT are assigned a creation key by entitlement system. The token may be created by either device manufacturer or owner which is combined with the device RFID. Whenever, owner changes for IoT device, token are changed by the owners where old token is provided so that it supersedes the access control and permission of previous owner.

III. Issues and Problems

There are many achievements and researches done in the field of IoT, still there are some open challenges that needs to be addressed. Now, threats to each layer of IoT are discussed.

A. Perception Layer Issues

This layer as already discussed contains sensor technologies like RFID [5] which are vulnerable to many threats which is discussed below.

- **Unauthorized Tag Access:** Large RFID systems lack proper authentication mechanism which can be exploited by the attacker. This can result is tag access by attacker without authorization and in worst case even deletion of data as well.
- **Tag Cloning:** Since tags are visible and can be read and modified by simple hacking techniques, any attacker can make a replica of the tag and thus compromising the system where it will be impossible to distinguish between real and fake tag.
- **RF Jamming:** Since RF signals are vulnerable to disruption, attackers can create DoS attack that adds noise signals thus compromising RFID tags.
- **Spoofing:** In spoofing attacker sends fake information to RFID systems and pretends to be actual source. Thus, attacker gets full access of that system and can even affect other devices.
- **Timing Attack:** Attacker can predict the encryption key by analyzing the time required to perform the encryption.

B. Network Layer Issues

This layer has Wireless Sensor Networks (WSN) which is responsible for transmitting information from sensor to destination securely. However, even this layer has security issues which are discussed below.

- **Denial of Service (DoS) Attack:** This is most dangerous attack in which attacker floods the network with useless lot of traffic that ultimately exhausts the object resources due to which network becomes unavailable to end users.
- **Man-in-the-Middle attack:** This is a form of eavesdropping attack where attacker can monitor private communication and even control a communication. He can even fake his identity and pretend to be actual user.
- **Malicious Code injection:** Attacker can inject some malicious code in the node that can result even in shutdown of the system or in some worst case get full control of the network.
- **Sleep Deprivation Attack:** The sensor nodes in IoT are battery powered and have a specific amount of battery life. To extend the battery, it follows sleep routines to extend battery life. Attacker can keep nodes awake which drains battery of the nodes causing shutdown.
- **Compatibility:** Due to heterogeneity of the network components, it gets difficult to use current network protocols since there is machine to machine communication.
- **Sinkhole Attack:** It is a kind of attack where adversary compromises a node and makes it look attractive to nearby nodes thus attracting data irrelevant to that nodes towards it causing network disruption.

C. Application Layer Issues

Since IoT still lacks global policies and standards that govern the device interaction, there are still many issues related to application layer security. Som

- **Sniffing Attack:** This is most common attack where attacker introduces a sniffer application into system that gains sensitive system information that can even corrupt the system.
- **Spear-Phishing Attack:** Here email spoofing is used to target victim in opening some infected mail mostly a high-ranking person and gains administrative privileges of the system thus getting full access of the system like HB Gary Hack.
- **Denial of Service (DoS) Attack:** Since DoS attacks have become very sophisticated where attacker even use smoke screens to pretend a normal behavior and breach defensive system. Thus attacker gets hands on all the unencrypted information.
- **User Interaction:** Different users have different levels of interaction and access. So, how users interact and amount of data to be revealed is another issue.

IV. Future Trends

IoT has seen rapid development in these years in different areas. Even analysts have predicted that number of IoT devices will cross 26 billion units by 2020. Considering growing popularity and acceptability of IoT among common masses security is a factor that must be dealt with to ensure users can use a secure IoT. Now, future direction for research to more secure IoT will be discussed.

- **Architecture Standards:** Current IoT implementation has different IoT devices that communicate to achieve a common goal, but these devices are working on different protocols. This creates problems in integration since sometimes there are compatibility issues and other problems which emphasizes need of a common standard that will be followed among all IoT devices [6]. This is the need of the hour as currently IoT is in a early stage and any change right now will be very easy to implement than in the later period when number of devices would have been increased manifold.
- **Identity Management:** This is very important as all first time connection exchange information that can be easily sniffed and thus compromising the full network. There should be proper security techniques like cryptography and other advanced techniques to prevent information theft.
- **Session Layer:** Since IOT architecture only has three layers and doesnt have any layer for managing sessions unlike OSI network model. Absence of the same can lead to devices taking malicious packets since it has no information of a session that can prevent an attacker from pretend to be source.
- **5G Protocol:** Since IoT is in its early stage, and we can expect its robust realization in coming years. So, we should design everything that is future ready [7]. Currently, IPv4 is being used that is almost exhausted and work is on to migrate the devices to IPv6 that can accommodate much larger number of devices. Moreover, 4G has speed range of 2-1000Mbps whereas IoT will need much higher speed range which 5G can provide. So, IoT framework should be developed to accommodate 5G protocols to enhance speed of device communication.

The current IoT architecture is still in its early stage with a lot of scope of improvement in areas of security, reliability and making it future ready. We discussed how current implementation is vulnerable at each layer which needs to be addressed. Also, to scale it well there is a need of standardization of protocols and architecture.

References

[1] Kevin Ashton, That Internet of things thing, It can be accessed at: http://www.rfidjournal.com/articles/view?4986

[2] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, ”Internet of things (IoT) security: Current status, challenges and prospective measures,” 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 336-341.

[3] M. Abomhara and G. M. Koien, ”Security and privacy in the Internet of Things: Current status and open issues,” in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[4] Alaba, Fadele Ayotunde, et al. ”Internet of Things security: A survey.” Journal of Network and Computer Applications 88 (2017): 10-28.

[5] Farooq, Muhammad Umar, et al. ”A critical analysis on the security concerns of internet of things (IoT).” International Journal of Computer Applications 111.7 (2015).

[6] M. Abomhara and G. M. Koien, ”Security and privacy in the Internet of Things: Current status and open issues,” in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[7] D. Singh, G. Tripathi, A.J. Jara, A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services, in Internet of Things (WF-IoT), 2014