A Survey on Security in IoT Networks: Solutions and Future Challenges

P.GOMATHI[1], R.PRABHU[2]

[1]*Assistant Professor, Dept. of Computer Science and Engineering, Hindusthan Institute of Technology, Tamilnadu, India.*
[2]*Assistant Professor, Dept of Computer Science and Engineering, Hindusthan Institute of Technology, Tamilnadu, India.*

---***---

Abstract - *Internet of things (IOT) Can be defined in many ways it encompasses many aspects of life such as connected homes, connected cities, connected cars and roads, roads to devices that track an individual's behavior. It is expected that one trillion Internet-connected devices will be available with mobile phones as the eyes and ears of the applications connecting all of those connected things. IoT made it possible for billions objects to communicate over worldwide over a public, private internet protocol network In 2010. In 2010 -11 the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. The essential idea of the Internet of Things (IoT) has been around for nearly two decades, and has attracted many researchers and industries because of its great estimated impact in improving our daily lives and society. As the use of IoT devices is increasing every moment several IoT vulnerabilities are introduced. The results and analysis indicate that massive deployment of IoT with an integration of new technologies are introducing new security challenges in IoT paradigm. In this paper, IoT security challenges and open issues are discussed which provides a ground for future research. Also it provides a review of security protocols that can be used for a range of IoT applications.*

Key Words: *Internet of Things, Security, threats, protocols*

1. IoT Introduction and Security Overview:

The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet framework. Typically, IoT is expected to offer advanced connectivity of devices and systems, and services that goes beyond M2M i.e. machine-to-machine(M2M) communications and covers a variety of protocols, various domains, and applications. The interconnection of all these embedded devices which also includes smart objects, is expected to lead in automation in nearly all fields enabling advanced applications like a Smart Grid. Objects or things communicate with each other and perform the required actions. Human does not need to interact with system. IoT system is made up of three components: sensor, actuator and connectivity devices. Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks. According to pane lists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below. First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer. Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud. Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information. This chapter deals with major issues, challenges and solutions for providing IoT security.

2. IoT Architectures and IoT Security:

The variety of IoT applications has resulted in various IoT architecture models. The basic model is with a three-layer architecture:

1. Perception layer

2. Network layer

3. Application layer.

The perception layer – also called the recognition layer – is the lowest layer of the conventional architecture of IoT. This layer is responsible for collecting data from "things" or the environment (such as Wireless Sensor Networks [WSN], heterogeneous devices, sensors, etc.) and processing them.

Some other models include one more layer: a support layer that lies between the application layer and network layer. For example, the ITU-T (International Telecommunications Union - Telecommunication Standardization Sector) suggests a layered IoT architecture that is composed of four layers (Fig. 1). The IOT application layer containing the application user interface is the top layer. The services and application support layer is the second layer from the top. The third layer is the network layer which contains the networking and transport capabilities. Finally, the lowest layer is the device layer, which contains gateways, sensors, RFID tags, etc. The security capabilities categorized into generic and specific (Fig. 1), are distributed along all four layers.

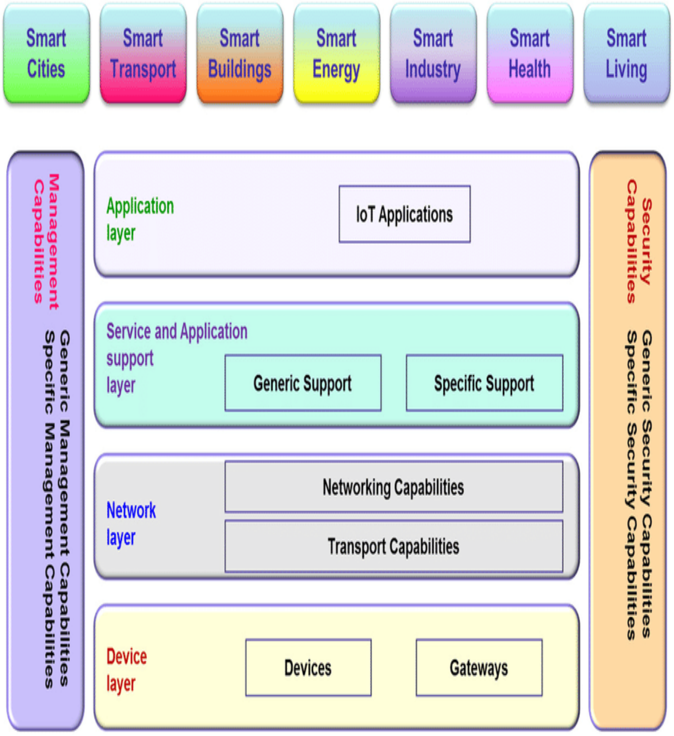

Fig 1: IoT Layered Architecture (Ref: 5)

The IoT European Research Cluster (IERC) adds more details to the ITU-T architecture of IoT by presenting the functions included in every layer (Fig. 2). For example, the third layer – the network and communication layer – includes the network and communication capabilities such as gateway, routing and addressing, energy optimization, QoS (Quality of Service), flow control and reliability, and error detection and correction. The security management functions listed on the right side include authorization, key exchange and management, trust, identity management and authentication.

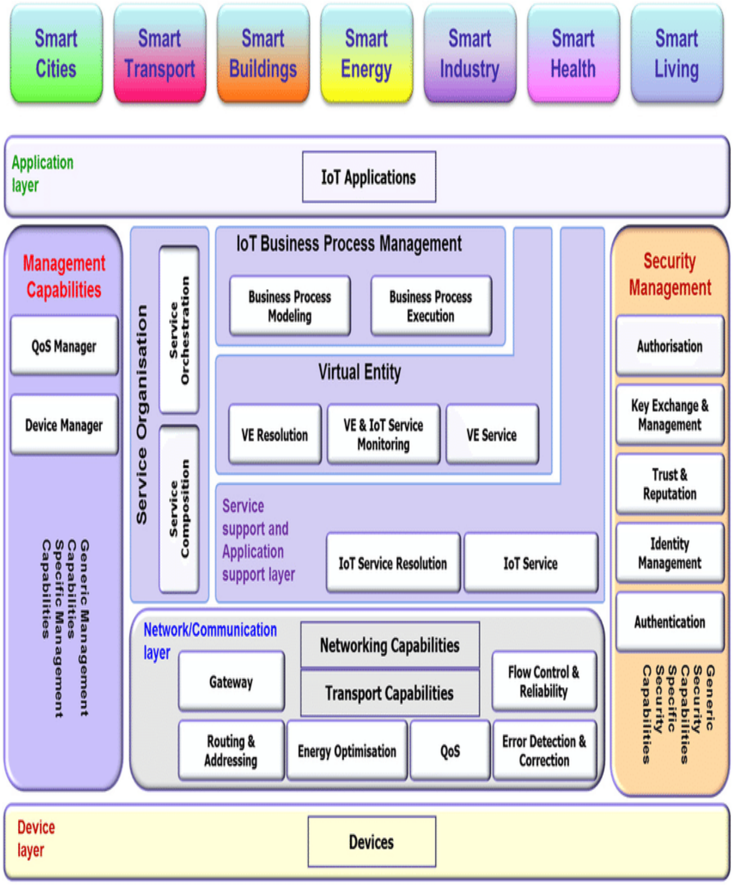

Fig 2: Detailed IoT Layered Architecture (Ref: 7)

2.1 Security in Short-Range Low Power IoT Networks

2.1.1 6LoWPAN Security

Low-data-rate, low-power wireless personal area networks (LR-WPANs) are based on IEEE 802.15.4 Standard for Low-Rate Wireless Networks. The standard is implemented by using several technologies such as 6LoWPAN (an IETF standard), Zigbee (Section 3.4), Z-Wave and EnOcean (building and home automation standard protocols), and SNAP (Simple Network Access Protocol). The idea of 6LoWPAN is a combination of IPv6 and IEEE 802.15.4. 6LoWPAN standard allows IPv6 to be used over 802.15.4 wireless networks. The Thread protocol for home automation devices also runs over 6LoWPAN. A 6LoWPAN network consists of one or more 6LoWPAN networks connected to the Internet through the edge router that controls flows incoming and outgoing from the 6LoWPAN. Within 6LoWPAN, devices do not use the IPv6 address or user datagram protocol (UDP) full header for transmissions as it remains at the edge router to communicate with the outside. Routing issues in 6LoWPAN are addressed by the IETF-ROLL Working Group in its design of RPL (a de facto routing protocol for Low-power and Lossy Networks [LLNs]). The security in the 6LoWPAN networks must limit data access only to authorized users, provide data integrity and be capable of detecting malicious intrusion. Since 6LoWPAN combines IEEE 802.15.4 and IPv6, an intrusion detection system is required to monitor the traffic of two sides. The lack of authentication at the 6LoWPAN layer, the best effort semantics for fragment transmissions, and scarce memory resources of the networked devices make the packet fragmentation mechanism of 6LoWPAN vulnerable. For example, an attacker can selectively prevent correct packet reassembly on a target node. Specifically, an attacker can mount attacks by only sending a single protocol-compliant 6LoWPAN fragment.

2.1.2 Security in RPL

IPv6 Routing Protocol for LLNs (RPL) is designed for routing IPv6 traffic in low-power networks implemented over 6LoWPAN with high or unpredictable amounts of packet loss. The RPL security utilizes a “Security” field after the 4-byte ICMPv6 message header. Information in this field indicates the level of security and the cryptography algorithm used to encrypt the message. RPL offers support for data authenticity, semantic security, protection against replay attacks, and confidentiality and key management. RPL attacks include selective forwarding, sinkhole, Sybil, Hello flooding, wormhole, black hole and denial of service attacks.

2.1.3 Security in Bluetooth Low Energy (BLE) BLE Protocol

BLE is a low-power version of the Bluetooth 2.4 GHz wireless communication protocol (Table 5). While the BLE data rate and radio range are lower than the same metrics in classic Bluetooth, BLE is designed for very low-power applications running off a coin battery (for example, the popular CR2032). The low-power and long battery life make it possible for BLE sensor devices to operate for many years without needing a new battery. To enhance security, the BLE version 4.2 introduces the new BLE Secure Connections pairing model. Let us briefly review the main

2.1.4 BLE security challenges

Passive eavesdropping, MITM attack, and identity tracking are some security challenges in BLE. Eavesdropping. The protection against passive eavesdropping can be based on encrypting communication with a key. While earlier versions of BLE (Bluetooth 4.1 or older) devices used easy-to-guess temporary keys to encrypt the link for the first time, BLE 4.2 uses the Federal Information Processing Standard (FIPS) compliant Elliptic Curve Diffie-Hellman (ECDH) algorithm for key generation (Diffie-Hellman Key—DHKey). Man-in-the-Middle (MITM) Attacks. Protection against MITM attacks is to ensure that the device the communication started with is indeed the intended device rather than an unauthorized device presenting as the intended one. LE Secure Connections pairing provides MITM protection by using the numeric comparison method. Privacy/Identity Tracking. As most of the BLE advertisement and data packets contain the source addresses of the devices that send the data, third-party devices could associate these addresses to the user identity and track the users. A frequent change of the private addresses so only the trusted parties could resolve them can serve as protection against this thread.

2.1.5 Zigbee Security

Zigbee Protocol. Zigbee is a wireless technology based on the IEEE 802.15.4 standard and used in various application areas, including home automation, smart energy, remote control and health care. It has a longer range than BLE and a lower over the air data rate than BLE. The Zigbee Alliance has developed the Zigbee Health Care Profile for secure non-critical patient monitoring, chronic disease management, drug administration (e.g. insulin pumps), and personal wellness monitoring. ISO/IEEE 11073 Personal Health Data standards-conformant devices (for example, blood pressure monitors, respirometers, pulse oximeters, ECGs, weight scales, and thermometers) are supported by Zigbee Security Features.

As with other IoT protocols, Zigbee has unavoidable trade-offs made to keep the devices low-cost, low-energy and highly compatible. To simplify the interoperability of devices, Zigbee establishes the same security level for all devices on a given network and all layers of a device. In addition, it assumes that “the layer that originates a frame is responsible for initially securing it”. Zigbee supports 128-bit AES encryption. Zigbee security includes an assumption that keys are securely stored, and devices are pre-loaded with symmetric keys so they have never to be transmitted unencrypted. However, when a non-preconfigured device joins a network, a single key may be sent unprotected to enable encrypted communication.

This one-time transmission of the unprotected key creates a short timeframe of exploitability during which the key could be sniffed by an attacker. The low-cost nature of some types of devices such as light switches or temperature sensors limits the device security features and it cannot be assumed that the hardware is built tamper-resistant. Hence, if an attacker obtains physical access to such a device, it may be possible to access the secret keying material and other privileged information as well as to access the security software and hardware. A paper published in 2016 explains the attack targeted on Philips Hue Light Bulbs implemented with the Zigbee standard. The light bulbs were infected with a worm/virus that gave the attackers the ability to turn them on and off. The worm was able to attack a light bulb from up to 400 meters away and then spread to nearby bulbs because Zigbee uses hard-coded skeleton keys. Zigbee Alliance in its response claimed that the vulnerability was not part of Zigbee standard, but rather an internal implementation error made by Philips. This allows us to generalize that while technology can be secure, its erroneous implementation could lead to security weaknesses.

2.1.6 RFID Security

Radio Frequency Identification (RFID) is the method of uniquely identifying "things" by transmitting their identity (usually a serial number) using radio waves. At a minimum, an RFID system consists of a tag, a reader, and an antenna. RFID tags storing identifiers and data are attached to devices for reading by an RFID reader. RFID tags can be active, passive, or assisted passive. Active RFID tags using their own power source can broadcast with a read range of up to 100 meters (Table 5). Passive tags are ideal for devices without batteries, as the ID is passively read by the reader. They have a read range from near contact and up to 25 meters and utilize the power of a reader's interrogation signals for any response. Assisted passive tags become active when an RFID reader is present. RFID technology is used not only in traditional applications such as asset or inventory tracking, but also in security services such as electronic passports and RFID-embedded credit cards. Even many pets – including my cat – have RFID chips in them. Some of the numerous RFID security and privacy threats are presented in Table 1 (adapted from Ref. 8).

Table 1: Security Threats in RFID Technology

Threats	Key Component	Security need
DoS attacks	RFID tags and reader communications DoS attacks RFID tags and reader	Encryption
Eavesdropping	User private data	Encryption
Skimming	User private	Shielding, blocking tags
Relay attack	Authentication result	Synchronization
Side-channel attack	User private data	Authentication
Hardware destruction	Tags	Protective electronic component
Software destruction	Commands	Key, password

2.1.7 Security in NFC

Near-Field Communication (NFC) is a subtype of RFID technology — High-Frequency (HF) RFID — and is based on 13.56 MHz, HF passive RFID/contactless card technology. As NFC devices must be in close proximity to each other (no further than a few centimetres in most cases), it makes NFC a popular choice for secure peer-to-peer communication between consumer devices such as smartphones. In contrast to typical RFID devices, an NFC device is able to act both as a reader and as a tag.

Threats	Key Component	Security need
Phishing attacks	Application processor	Interfaces authentication
User tracking	User privacy	Random UIDs
Relay attacks	Tag/reader	Synchronization
Data corruption and manipulation	User data	Use of secure channels
Eavesdropping	User data	Use of secure channels
Interception attacks	User data	Devices should be in an active-passive pairing
Malicious host	Application processor	Interfaces authentication

Table 2: Security Risks and Their Mitigation in NFC.

NFC security threats and protection solutions are shown in Table 2 (adapted from Ref.9)

2.2 Security in the Future IoT Systems

This paper considered the current status of the main IoT security domains in the sections above. So the current section will discuss the trends in IoT security development and briefly consider some emerging technologies that can make the next generation IoT more secure. Also which new security features and technologies are required to address these limitations in the future will be reviewed.

Future IoT systems should be able to quickly and appropriately respond to threats and attacks, incorporate and learn from new threat information, and develop and enact thread mitigation plans. The capability to cooperatively diagnose problems and implement security plans for various subsystems in the system, which may be owned by different entities, is also required. Future IoT systems should also be able to ensure controllable data ownership across enterprise boundaries. To preserve the privacy of customers and/or enterprises while processing a large amount of data, new data analytics algorithms and new cryptographic methods, such as homomorphic or searchable encryption (Sections 4.1 and 4.2), are needed. Sharing threat intelligence information by different systems enables cooperative security measures that are capable of realizing more cohesive knowledge of the current and future attacks.

2.3 Next Generation IoT Security: Data Confidentiality

2.3.1 Homomorphic Encryption

Homomorphic encryption schemes make it possible to perform mathematical operations on ciphertexts. As a result, using fully homomorphic encryption (FHE) data analytics on encrypted data or searching on encrypted data can be performed without revealing search patterns and without actually seeing the original information. An example of the use case for FHE is an analysis of private healthcare IoT data to study the opioid crisis so that the data owners can be assured of data privacy.

2.3.2 Searchable Encryption

Searchable encryption schemes allow a storage provider to search for keywords or patterns in encrypted data. While keyword searches can be performed, the stored data cannot be decrypted and it is not possible to gain any knowledge of the underlying plaintext.

2.4 Next Generation IoT Security: Trust

2.4.1 Blockchain and IoT

Trust in Transactions Blockchain-based protocols that are gaining popularity can address the challenge of establishing trust. One of the key building blocks of future IoT trust infrastructures can be smart contracts based on blockchains, as they are a prerequisite for business-critical interaction between devices without direct human interaction. However, blockchains require computational resources and have high bandwidth overhead. This limits their use in IoT and new lightweight blockchain-based technologies are needed.

2.5 Next Generation IoT Security: Privacy

2.5.1 Privacy through Data Usage Control

Data usage control is an extension of traditional access control concepts. Future data usage control technologies will extend traditional access control concepts to track and label data as it is processed by various systems. They will define fine-granular usage restrictions in order to enforce privacy properties over large data sets while still allowing for running learning algorithms and analytics over them.

3. CONCLUSION

Today IOT is being implemented everywhere which is of human concern like Smart city, smart environment, security and emergencies, smart business process, smart agriculture, domestic and home automation and healthcare. In this paper, we presented the overview of IoT security threats, solutions for addressing them, and new evolving technologies. It shows the paramount importance of security in developing viable IoT solutions.

REFERENCES

[1] . Mr.K.Muruganandam, Dr.B.Balamurugan, and Dr.Sibaram Khara (2018), “Design Of Wireless Sensor Networks For IOT Application : A Challenges and survey” , International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 7 Issue 3 March 2018, Page No. 23790-23795.

[2] 2. Mikhail Gloukhovtsev (2018),” IOT SECURITY: CHALLENGES, SOLUTIONS & FUTURE PROSPECTS”, Knowledge Sharing Article © 2018 Dell Inc.

[3] 3. Suraj Choudhari , Tejas Rasal , Shubham Suryawanshi , Mayur Mane , Prof. Satish Yedge (2017) , “Survey Paper on Internet of Things: IoT”, IJESC ,Volume 7 Issue No.4.

[4] 4. Nunberg, G. (2012), The Advent of the Internet: 12th April, Courses.

[5] 5. International Telecommunication Union – Telecommunication Sector, Series Y: Global Information Infrastructure, Internet Protocol Aspects and next Generation Networks - Frameworks and functional architecture models - Overview of the Internet of things, Y.2060", June 2012.

[6] 6. IoT 2020: Smart and secure IoT platform. IEC White Paper. http://www.iec.ch/whitepaper/iotplatform

[7] 7. IERC Cluster SRIA 2014 – Internet of Things

[8] 8. 7. A. Khattab et al. RFID Security, Analog Circuits and Signal Processing. Springer International Publishing AG, pp.27-40, 2017.

[9] 9. K. Laeeq and J. A. Shamsi. A Study of Security Issues, Vulnerabilities, and Challenges in the Internet of Things. In Securing Cyber-Physical Systems. Taylor and Francis. Oct 2015.