***HIGHLIGHTING THE VARIOUS SECURITY ISSUES AND SOLUTIONS RELATED TO PERCEPTION LAYER.***

Jittin Mathew

1. **Introduction**

Is the Internet of Things (IoT) a specific device or technology? The answer is No, the IoT enables the connectivity of many things using an inter-working of different technologies. The purpose of IoT system is to observe the surrounding in which it is placed, to enable and assist, or to automate a response to changes to that system’s environment. By doing this, it enables the best response to an environmental change by providing responsive services particular to the take of the user at the receiving end. Internet of Things in short referred is as ‘IoT.’ It is an ecosystem of a network of interconnected things i.e. devices, objects capable of communicating with each other with the help of the embedded technologies inbuilt in it. This new technology with the help of electronics, software, sensors, actuators, unique barcode and identifiers collect the data from the environment surrounding it and exchange it with each other using the global system of interconnected computer networks commonly known as the Internet with the help of the unique Internet Protocol address (IP addresses) assigned to it [1]. Today we are living in the age of digital revolution where communicating among people and getting everything online is normal. Various processes and technologies have been developed to reduce manual intervention and involve more artificial intervention for collecting, processing and execution of data leading to a large amount of information gathering from the environment, saving of time, energy, and resources and delivering of a more efficient, accurate performance. IoT is the one such fruit of this digital revolution. Though, IoT has come to existence recently but it has managed to grow rapidly and emerge itself as the new ‘IT’ of the fast- and ever-growing digital era. The IoT with its rapid growth is also affected with a lot of issues, mainly in terms of security. IoT- based applications have found their way in the health, military, commercial, education and even in research and development field. According to the experts, there are 127 IoT devices getting online every second. Around 35 million number IoT devices will be on the web by the end of 2021, which will increase to 75 billion by 2025 [2]. In any IoT system, the importance is given to data or information collection. If the data or information is accurately collected then there will not be any absurdity in the final result. The acquisition and collection of data happens in the Perception layer in the IoT architecture. This makes the perception layer very important component of any IoT system. In this paper, we will analyze the perception layer to understand the technologies it uses and the security breaches if faces and some solutions suggested to have a safe and secure data been transmitted to the perception layer. We also briefly understand the evolution of technology to its present form the Internet of Things (IoT) and various architectural progress in the design of the IoT architecture. The main objective of this paper is highlighting the various security issues and solutions related to perception layer.

* 1. **Objectives**

The perception layer plays an important role in the IoT systems, because it where the first contact with the data is made and the actual data acquisition takes place. Moreover, the perception layer is vulnerable to various types of security attack. Hence, it is very much necessary to design a safe mechanism to secure communication in the IoT-enabled perception layer.

The main motivations of this paper are as follows.

Understanding the importance of Internet of Things (IoT).

Reviewing the various growth in the architecture of IoT.

Understanding the Perception Layer.

Highlighting the various security issues and solutions related to perception layer.

* 1. **Structure of the Paper**

Section 2 introduces the concept of the evolution of Internet of Things (IoT). In Section 3, we review the various architectural design of IoT and the specially the perception layer. The analyses of the security issues and solutions related to the perception layer are presented in Section 4.

1. **Evolution: A step by step progress of technology towards Internet of Things (IoT)**

The culmination of two hundred years of evolution within the information technologies is the Internet of Things (IoT). From the Figure 1 [12], It is understood that the most important milestone within the IoT is the invention of the Internet and the World Wide Web (WWW). The IoT is a relatively new idea with the initial concept introduced only in the year 1999. Its development cycle is just 15-20 years but has emerged as the dominant force to be termed as the new ‘IT’ i.e. new age of Information Technology. Though the IoT was introduced to the consumer only in year 2014, it has developed significantly with creation of thousands of products. A survey by International Data Corporation (IDC) (<https://www.idc.com/>) estimates 41.6 billion IoT connected devices or things generating 79.4 zettabytes (ZB) of data by the year 2025. In the figure 1, the development leading to the emergence of IoT is depicted. The table shows particularly the devices which are now used or the ideas that are currently implemented in the development of IoT devices to name a few Barcode and RFID tags are used in the Perception Layer of IoT architecture to collect data from the IoT enabled devices.

|  |  |  |
| --- | --- | --- |
| **YEAR** | **DEVELOPMENT** | **RESPONSIBLE** |
| 1830 | First Wireless Technology- Electronic telegram | Baron Schilling |
| 1876 | First Wire conversation-  Telephone | Alexander Graham Bell |
| 1927 | Frist Television- capturing moving images, transmitting them as radio waves and converting them back to images to display on a screen | Philip Taylor Farnsworth |
| 1949 | Patented the Barcode | Norman Joseph Woodland |
| 1955 | First wearable Computer | Edward Throp |
| 1968 | Creation of ARPANET, predecessor to INTERNET | United States Defence department |
| 1969 | Patented the passive RFID tag | Mario Cardullo |
| 1991 | Birth of World Wide Web | |
| Concept of ‘Ubiquitous Computing’ published in Scientific American Journal. | Mark Weiser |
| 1994 | Development of a wearable wireless Webcam | Steve Mann |
| 1999 | The term ‘Internet of Things’ first coined | Kevin Ashton |
| The book ‘When Things Start to Think’ published | Neil Gershenford |
| 2006 | IoT formally recognised | The European Union |
| 2008 | Announced ‘The Birth if IoT’ | CISCO |
| 2011 | Launch of IPV6 protocol and Raspberry Pi microcontroller |  |
| 2014 | IoT presented to the consumer market |  |
| 2017 | Development and Implementation of Security strategies and laws regarding IoT |  |

Figure 1: The table shows the important developments leading to the evolution of IoT.

1. **Various Architectural Design of IoT**

In the architectural design of IoT we can see a technological revolution. The design represents a combination of both computing and communication architecture along with some additional distinguishing features of its own. So, IoT is not a direct extension of these networks but an adaptation of the features of both the Internet and Telecommunications Network with some peculiar distinguishable features of its own [14]. The traditional three-layered Architecture of IoT consists of the application layer, network layer and the perception layer. This architecture has been designed and implemented in a number of systems. Though this architecture is simple, behind the simplicity of this multi-layered architecture there are diverse and complex operations been carried out in the some of the layers. In the network layer, along with the specification of the best route to transmit data it has to also provide data services such as data aggregation, computing, etc. Whereas in the application layer, data services like data mining, data analytics are done along with its normal services to customers and devices. To avoid these multi-complex operations carried by some layer the concept of Service-oriented Architectures (SoA) has been developed. In the SoA, different functional units (services) of the network and application layer connect to the traditional architecture through interfaces and protocols to form a new layer, called the service layer or the interface layer or middle layer. Thus, in the SoA- based IoT architecture, along with the three layers of the traditional three-layered architecture the service layer is added as the fourth layer. Further in some architectures, the service layer is subdivided into two sub-layers service composition and service management. There is also some architecture in which a new business layer is extracted from the application layer. The business layer is placed above the application layer to provide complex service requests [3]. A new five- layered architecture is need the of hour. Through analysis it is found that the the other two architectures sometimes fail to express the whole features and connotation of the IoT. So, combining the technological architecture of the Internet and the logical structure of Telecommunications Management Network, combined with the specific features of the traditional IoT architecture the concept of a new architecture is developed. With the five layers been the Business Layer, Application Layer, Processing Layer, Transport Layer and the Perception Layer [14].

Business layer

Application layer

Application layer

Application layer

Service layer

Network layer

Processing layer

Network layer

Perception layer

Figure a: Three- Layered architecture of IoT

Transport layer

Perception layer

Figure b: SoA- based IoT architecture

Perception layer

Figure c: New architecture of IoT

Figure 2: Various Architectural design of IoT

* 1. **Understanding of the Perception layer**

Perception layer collects information by perceiving the physical properties of objects such as the temperature, location and so on by the help of sensors namely infrared sensors, RFID, 2-D barcode, etc. and then converts these analog signals to digital signals for further transmission to network layer. The Perception layer can be further categorised into Perception nodes and Perception Network. The perception node does the data acquisition and data control while the perception network transmits the collected data to the gateway or else conveys the control instruction to the controller. The technologies used in this layer include RFID, WSNs, RSN, GPS, Barcode, etc [7].

NFC

IrDA

DASH7

FireWire

ZigBee

UWB

BTLE

6lowPAN

Perception (Physical Sensing) Layer

Tag-types RFID

QR

Bar code: 2D, 3D

QR code

Gyroscope

Photo-

Electric

Piezo-

Electric

Solid State

Electro-

Mechanical

Electro-

Chemical

Speedo-

meter

Accelero-

meter

Catalytic

Photo-

ionization

Infra-Red

GPS

Tempera-

ture

Humidity

Pressure

Sweat

ECG

EEG

Respiratory

Pulse

SPO2

Tilt

Pedometer

EMG

INSTEON

Wireless

USB

IEEE

P1906.1

NAN

LF

HF

UHF

Sensor based Networks

Sensor-types / Actuators

Sensor-types/ Actuators

|  |
| --- |
| LogoQ |
| iQR |
| SQRC |

Figure 3: Various Sensor- types Actuators and Sensor based Networks technologies used in the Perception Layer [15]

**3.1.1** **Technologies used in Perception Layer**

The technologies used in this layer are sensing technology, RFID technology, Global Positioning System, etc. Some of the technologies are explained in detail as follows

**RFID**

The Radio frequency identification system is a technology uses radio frequency transmitted wireless communication to send and receive data. It has two components: RFID tags and RFID reader. Using the integrated RFID antennas these two technologies communicate with each other [8]. It is generally a non-contact communication technology. Its working can be explained as follows the RFID- based system comprises of RFID tag, RFID reader, and antenna. A microchip attached to the antenna is the RFID tag. Each tag with a unique identification number is attached in an object. The RFID reader identifies the object and collects the information from the RFID tag using appropriate signals, which is transmitted by the antenna. Few advantages

RFID technology does fast scanning, it is durable, reusable, has a large storing capacity, low cost. RFID is mainly used for object identification.

**WSN**

Wireless Sensor Networks are independent node structures which can communicate wirelessly only over a limited bandwidth and frequency. The nodes comprise of the sensors, microcontroller, battery, transceiver and memory. The communication in WSN takes places through multi-hop information relay due to the limited communication range of each WSN sensor node. The use of wireless radio transmitters-receivers for the transmission of data between the nodes make the communication network dynamic in nature [8]. Through WSN, the status of the devices can be tracked, it is scalable, it allows dynamic reconfiguration, it is reliable, consumes low energy. It is mainly used to perceive the real-world physical parameters associated with the surrounding environment [3].

**RSN**

RSN is an integration of RFID system and the sensor network. To identify and track the status of the objects RSN technology uses the sensor network with RFID system. It has a RFID-based sensing device. The RFID reader work as sink node to generate data and provide power for network operations [3].

**Barcode**

In one-dimensional code, this technology stores the information in the form of black lines and white spacings. The lines and spacings are of different widths and arranged with special encoding rules. In two-dimensional, the code are recorded by the help of black and white pixels laid on the plane. The black pixel represents a binary of 1 while pixel represent binary 0. In barcode, the two-dimensional code gives high information content, high reliability, high robustness [3].

1. **Security**

The IoT been a recent and emerging development in the field of Information Technology. It uses a multitude of communication protocols implemented over a varied variety of devices, so it has to face a lot of major issues, the most significant been the security vulnerabilities. The reason for it been that the security in IoT devices has been a developmental afterthought. IoT uses the sensor networks, mobile communications and the Internet to connect the IoT enabled devices, so it faces also the security issues related to these systems. It also has security issues particularly related to it functions. The security issues of IoT basically comes from itself or from the multi heterogeneous network related technologies it uses. In this paper, we will have a better understanding to security issues faced by the Perception layer. Perception layer as seen in the above section of Architecture design, is the first and foremost layer of the IoT Architecture. It collects the data from the IoT enabled devices and transmits to the technology. So, if here the data is not collected accurately or the data is manipulated the entire process will be corrupted. Hence it is very important to secure the Perception layer. So, in next section we will analyse the security issues in more detailed way in of perception layer specially in its perception nodes and perception network [7].

* 1. **Security issues and its solution in the Perception layer**

All the data in the IoT system is been collected from the environment using various collecting and control modules present in the perception layer. The perception layer consists of two parts namely the perception nodes and the perception network. The perception node are the sensors, the controllers, etc. which are used for collecting the data whereas the perception network helps the data to communicate with the gateways and controller in the transportation network [1]. In Figure 4 [13], we can look at the pictorial representation of the security architecture of the Perception Layer. The technologies involved at the Perception Layer are RFID, WSNs, RSN, GPS, etc. so regarding the security issues of perception layer we have analyse these technologies. In the figure 3, there is in detail, the explanation of the issues and solution related to these technologies mentioned in a tabular form [7].

Fusion security

Routing Protocol Security

Protocol Security

Perception

Micro-electromechanical systems (MEMS) Security

Nano-electromechanical systems

(NEMS) Security

Global Positioning System (GPS) technology Security

Network

Sensor +

RFID reader Security

RFID +

WSN

Security

Base station Security

Cryptographic algorithms

Reader Security

Key management

Tag counterfeit Security

Perception

Sensor + Tag security

Node

Sensor tag security management

Tag encode Security

Node trust management

RFID security WSN security RSN security

Figure 4: Typical IoT Security architecture of the Perception Layer

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. no** | **FEATURES AND ISSUES IN RFID TAGS** | **TECHNOLOGIES** | **SOLUTIONS** | **EXPLANATION** |
| 1. | Presence of a variety of sensor devices | Application of Uniform encoding for RFID tag | Uniform encoding | EPC technique is supported by European while UID technique is used in Japan |
| 2. | Presence of multiple tags in one reader’s working scope | Conflict collision prevention in RFID Tags’ collision | Anti-collision algorithm | Slot ALOHA, improved slot ALOHA, GBT, PGT, etc. |
| Readers’ collision | Scope-based solutions | Avoids overlap of reader working scope |
| Time-based solutions | Prevents readers from sending signals simultaneously |
| 3. | Limitation of resources such as less storage capacity, weak computational capabilities, easily crack able tags | Privacy protection on RFID | Physical-based schemes | Deactivation kill command, block tags, clip tags, pseudonyms tags, Faraday nets, signal interference and antenna energy analysis |
| Password-based schemes | Hash locks, random hask locks, hash chain, anonymous ID, re-encryption |
| Compromising solution | Store less important information in RFID tag, and store important information in the up-level service |
| 4. | Short password-based security mechanisms, easily forgery tag, tag replication, eavesdropping and retransmission | Trust Management in RFID | RFID-CoA | Unique ‘RFID-fingerprint’ for the RFID tag, cheap hardware technology |
| RFID security protocol | RFID private authentication protocol, RWP, AFMAP, ultralight weight RFID mutual authentication protocol, etc |
| Digital signature technology | For Low-cost GPS system provide lightweight authentication protocol while Tag replication prevention, data authentication provides efficient data protection |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. no** | **FEATURES AND ISSUES IN WSN** | **TECHNOLOGIES** | **SOLUTIONS** | **EXPLANATION** |
| 1. | Key distribution, including the distribution of the public key and the secret key, is to ensure key to be transported and distributed securely to legitimate users | Key management in WSN | Key broadcast distribution | Security communications between nodes in the same group |
| Distribution of node master key | Saved into the node before deployment in the form of pre-distribution |
| Distribution of the key shared between nodes | Communication between any pair of nodes protection, security communications between adjacent nodes |
| Symmetric key algorithms | SPINS, the famous random pre-distribution key scheme, q-composite, Pre-distribution matrix key scheme |
| 2. | Data security with limited computing power and storage space | Cryptographic algorithms in WSN | Symmetric encryption | Inconvenient digital signatures, message authentication, RC4, IDEA, RC5, TinySec |
| Public-key encryption | Rabin’s scheme, NtruEncrypt, elliptic curve cryptography, etc. |
| 3. | Limitation of power, computing ability and storage capacity, attacks towards routing protocol | Secure routing protocol in WSN | Secure routing protocols designed specially for WSN | Authentication protocols should discuss and verify the security of themselves in detail and should take energy management issues of wireless sensor network into consideration carefully |
| 4. | Limitation of resources, easy capture of nodes, and unique communication mode | Trust management in WSN | Measurement, evaluation, relationship formalization, formal derivation of trust | Update of trust, cooperation of all nodes, trade-off between limited resources and network security |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. no** | **FEATURES AND ISSUES IN HETEROGENEOUS INTEGRATION TECHNOLOGY** | **TECHNOLOGIES** | **SOLUTIONS** | **EXPLANATION** |
| 1. | Differences of storage formats, information access formats, security control mechanisms, data processing methods and data filtering aggregation | Heterogeneous integration technology | WSNs solutions | Random-intensive distributed low-cost static sensor nodes |
| RFID solutions | Heterogeneous integration technology |
| WSN in IoT solutions | Multi-hop, intelligent RFID reader/tag, potential privacy exposure, compatibility issues, unified data encoding standard and item information exchange protocol |

Figure 5: Issues and Solutions to the Security of IoT at Perception Layer

1. **Discussion**

Many objects cannot be perceived directly, they have to be implanted with microchip. Through these chips the temperature, speed, etc. are sensed and processed into information. The technique used for making the chips small enough to be implanted into objects as tiny as sand is called Nanotechnology. Further research studies in the field of nanotechnology and embedded intelligence technology is the key for the development of new ideas in the Perception Layer.

The Perception Layer is also challenged and vulnerable to attacks from the ‘Shadow IoT devices’ ( devices which in active use without the knowledge of the organization’s network) been present in the network. These shadow IoT devices include personal computers, to personal health monitors and other smart devices. A recent survey by IT security company Infoblox (<https://www.infoblox.com>) showed that there are conducted a survey over 1,000 IT leaders in the United States, United Kingdom, Germany, and the UAE to understand the prevalence of shadow IoT networks within organizations. The results shared showed that 78% of respondents had over 1,000 shadow IoT devices connected in their enterprise networks on a typical day, while 28% had between 1000 to 2000 devices in the network. Close to half (48%) of the organizations had between 2000 and 10000 devices connected to the corporate network. Further, exploring the world of shadow IoT networks involving a variety of devices, they found that49% and 47% respectively come from Fitness trackers such as Fitbit, Gear Fit and digital assistants such as Amazon Alexa and Google Home, while Smart TVs following at 46%, Smart Kitchen appliances like smart microwaves contribute to 33%. Gaming consoles such as Xboxes and PlayStations make up 30% of shadow IoT devices.

1. **Conclusion**

In this paper, we have seen a. step by step progress of technology towards Internet of Things (IoT). The emergence of IoT as the new ‘IT’ of the digital evolution though been a recent concept with the development cycle of only 15 to 20 years. The evolution of the various architectural design of IoT is stressed upon. In detail the Perception layer of the IoT is analysed with its understanding, the technologies used and the security issues faced in the layer and the solutions proposed to tackle it.

Further research studies in the field of nanotechnology and embedded intelligence technology is required to bring in better security measures in the devices itself in case of ‘Shadow IoT devices’ than to depend on the security solutions offered at the architectural level.

**References**

1. H. Zhao. Yuchen Yang, Longfei Wu, Guisheng Yin, and Lijie Li, “A Survey on Security and Privacy Issues in Internet-of-Things,” 2015 10th Int. Conf. Internet Technol. Secur. Trans., vol. 4, no. 5, pp. 202–207, 2015.
2. [The IoT Rundown For 2020: Stats, Risks, and Solutions -- Security Today](https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2),https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020. aspx?Page=2. Accessed on November.2020.
3. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017.
4. A. Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Futur. Gener. Comput. Syst., 2018.
5. A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” Digit. Commun. Networks, vol. 4, no. 2, pp. 118–137, 2018.
6. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: A survey,” J. Netw. Comput. Appl., vol. 88, no. December 2016, pp. 10–28, 2017.
7. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” W. Networks, vol. 20, no. 8, pp. 2481-2501, November 2014.
8. K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali and E. Benlahmar, “Perception layer security in the internet of things,” Procedia Computer Science, vol. 175, pp. 591-596, 2020.
9. K. S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain and K. K. Mahapatra, “Security Enhancements to System on Chip Devices for IoT Perception Layer,” IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pp. 151–156, 2017.
10. M. Weiser, “The Computer for the 21st Century,” Scientific American, vol. 265, no. 3, pp. 94-104, September 1991.
11. R. Ande, B. Adebisi, M. Hammoudeh and J. Saleem, “Internet of Things: Evolution and Technologies from a Security Perspective,” Sustainable Cities and Society, vol. 54, Article no. 101728, March 2020.
12. M. B. M. Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” Computer Networks, vol. 148, pp. 283-294, January 2019.
13. M. Wu, T. J. Lu, F. Y. Ling, J. Sun and H. Du, “Research on the architecture of Internet of Things,” Advanced Computer Theory and Engineering (ICACTE), vol. 5, pp. 484-487, September 2010.
14. P. P. Ray, “A survey on Internet of Things architectures,” Journal of King Saud University- Computer and Information Sciences, vol. 30, no. 3, pp. 291-319, July 2018.