International Journal of Engineering & Technology, 7 (2) (2018) 544-550

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i2.9504
Research paper

Deployment of IoT based smart environment : key issues and challenges

Deepti Sehrawat [1] *, Nasib Singh Gill [1]

[1] Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana (India)
**Corresponding author E-mail: dips.scorpio@gmail.com*

Abstract

The Internet of Things (IoT) is viewed as a dynamic technological revolution representing future communications and computing in several areas. It introduces physical objects in the sphere of cyber world. IoT is not about a single technology but various complementary technological developments which provides ways to bridge the gap between the real world and the virtual world. A number of wireless sensor technologies are implemented in IoT viz. RFID, ZigBee, actuators, WiFi and wireless sensor networks (WSNs). This paper presents various key technologies involved in IoT and its detailed architecture. IoT architecture explains function of each layer with respect to the technologies and the devices that surround each layer. Each layer has its specific security issues. This paper presents various security threats related to each IoT layer and the specific security requirements. Information security, data protection, and user's privacy are among important key areas in IoT. This paper in the nutshell presents new challenges posed by IoT so that further work can be undertaken in creating a robust, efficient and smart environment for IoT based applications.

Keywords: *IoT architecture; Key Technologies; Security; Threats; Threats Prevention.*

1. Introduction

In the present digital world IoT is considered as a buzzword which is coined from two words, “Internet” and “Things”. In early 1980's, a Coke machine at Melon University was the first Internet appliance that was connected to the Internet by the programmers. In 1999, Kevin Auston gave the term “Internet of Things” and IoT concept first time became very popular.

Now-a-days the wireless technologies are playing a vital role in our lives. Various tagging technologies including NFC, RFID, and 2D barcode are used to identify physical objects over the internet. These wireless tagging technologies are the key technologies in IoT. 2D barcodes have less complexity and lower development cost due to which 2D barcodes turn out to be a primary tool to create a linkage between different physical objects and their virtual representation. Spreading unwanted and unidentified data over the Internet is known as Spamming. Authors in [1] discussed different ways of spamming the IoT and proposed a possible solution to prevent from spamming. They proposed that IoT spamming can be addressed using digital signatures. Web spammers using 2D barcode technology can flood the physical side of IoT. They can get unsolicited content over the Internet either to change the contents or for misusing the information. Using digital signatures (ECDSA) can help to overcome the spamming of IoT [1].

Moving from static web pages to dynamic social networking web, there is an increase in the on-demand data generated through queries. Paper [2] presents a cloud-centric vision for IoT implementation. Authors in this paper proposed a cloud-centric implementation using interface between public and private Clouds. The proposed implementation used Aneka and concludes that WSN, Internet and distributed computing should be converged.

Various technologies are taking part in the IoT to make it successful. Wireless Area Network (WAN) or WLAN made it possible to execute operations for a long duration without any human intervention.

With the advancement of this new technology that improves social efficiency have side effects also in the form of information security and privacy [3].

Smart health is an area of IoT which requires continuous fine-grained information from sensors attached to patients. In such applications, a human body is providing a rich source of information like location, time, behavior, personal habits, and preferences of individuals. This information is then using cloud services thus making privacy critical aspect of IoT. Along with the data acquisition and data management, easy to use tools should be provided to users for better privacy [4].

Data protection and user’s privacy are two important key areas in IOT. Authors in [5], considers IoT security issues to the national level because of wide application areas of IoT including smart government, smart city, intellectual property and other social services. IoT includes everything to communicate over sensor network anywhere. This inclusion of everything increases the storage demand and network load exponentially. Technology development and new applications of business development affect IoT positively. An IoT architecture is proposed by authors in [6] which addresses scalability, reliability and interoperability. Proposed architecture includes five layers, the fifth extra layer is business layer along with the four common layers: Perception layer, Network layer, Support layer and application layer.

Unique identification and virtual representation of objects are offered in IoT. Authors in [7] proposed a futuristic architecture by integrating security and privacy. Authors proposed to make use of human inputs without their participation. A similar study in [8] presents a IoT architecture for industrial environments and smart building. Proposed architecture is based on OPC.NET specifications.

In this paper, various security issues related to IoT architecture and their effect on different layers are presented.

Rest of the paper is organized as: Section 2 covers various key technologies involved in IoT environment. In section 3, architecture of IoT is presented and various threats to each IoT layer are summarized along with their possible solutions. Section 4 concludes our findings.

2. IoT key technologies

RFID, Bluetooth, WiFi, ZigBee, Nanotechnology, Tagging technologies like NFC (Near Filed Communication), Actuators and Wireless Sensor Networks (WSN) are among the key technologies of IoT. Among them, RFID is the foundation and networking core of IoT [4]. In this section, the technologies involved in the smart environment are presented. These are:

2.1. Radio frequency identification (RFID)

RFID is a reliable, efficient, secure and cost-effective wireless system that uses radio waves so that a serial number as an identity of an object is transmitted. RFID in IoT based applications play an important role. RFID Tags are of two types; first is active RFID Tags that get power from batteries and the second type of RFID Tags do not use the onboard power supply and these are known as passive RFID Tags [9].

2.2. Internet protocol (IP)

Internet Protocol (IP) was devolved in the 1970s and is now used as a primary network protocol. It is a numerical label, assigned to the networking devices which uses Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Two versions of IP are available and these are: IPv4 and IPv6. Each of these versions defines different IP addresses.

2.3. Electronic product code (EPC)

The EPC is designed as a universal identifier that provides a unique identity for every physical object anywhere in the world, for all time. It is a 64/ 98-bit code that is electronically recorded on RFID tag. It was Auto-ID centre that developed EPC in the year 1999. EPC can store different information like EPC type, unique serial number of the product, manufacturer, and specifications of EPC [4].

2.4. Barcode

Barcode uses a varying width of bars and spaces to encode numbers and letters. These Barcodes are attached to items that have item information and are in optical machine-readable form. Numeric, Alpha Numeric and 2 Dimensional barcodes are three different types of Barcodes. Cameras and Laser-scanners are two devices that are used by these barcodes.

2.5. Wireless fidelity (Wi-Fi)

Wi-Fi is a wireless technology that allows communication among computers and other devices over a network. Wi-Fi integrates into a number of daily usable devices including handhelds and consumer Electronic devices boost the Wi-Fi adoption to an extent that it is nearly a default in these devices.

2.6. Bluetooth

Bluetooth is a short-range, inexpensive radio technology that eliminated the need for connection based connectivity. This wireless technology allows communication among devices within an effective range of 10 to 100 meters.

2.7. ZigBee

ZigBee Alliance in 2001 created a ZigBee protocol for enhancing wireless sensor network features. This protocol offers low cost, low power, reliable short transmission range, around 100 meters. It offers a bandwidth of around 250kbps. This protocol is based on the IEEE 802.15.4 standard [10].

2.8. Near field communication (NFC)

Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone. NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smartcards and allow mobile payment to replace/supplement these systems. NFC offers a short-range wireless communication at 13.56 MHz, usually within a distance of 4 cm. Its main advantage is that it works even in a dirty environment without requiring line of sight. It makes transactions, connection and digital exchange simpler and easier.

2.9. Actuators

An actuator is a component of a machine that is responsible for moving and controlling a mechanism or system, for example by opening a valve. In simple terms, it is a "mover". Actuators convert energy into motion using electric current, hydraulic fluid or some other power source. It can create different motions including linear motion, oscillatory motion or rotary motion. An actuator is the mechanism by which a control system acts upon an environment.

2.10. Wireless sensor networks (WSN)

WSN is an important IoT element in which there are a number of independent devices spatially distributed over a network. Sensors are used by the devices in IoT environment that monitors the different conditions like temperature, pressure on the object, the motion of an object, vibrations, etc. These Sensors are inserted on or to IoT objects in order to capture information about that object like sensors attached to chairs monitor pressure and respond accordingly [4].
Objects in IoT use different technologies in a different environment so as to build a smart environment. This results in a complicated dynamic system and requires a platform-independent WSN infrastructure. This large-scale sensor network must be capable of data management, information processing, and data analysis.

3. IoT architecture

IoT concept relies on a layered architecture. In IoT architecture, there are four layers and these are: Perception layer, Network layer, Session layer and Application layer. Each layer is defining its functionality which is different from other layers. Participating devices, diverse technologies, and services it provides defines each layer. Threats to each layer of IoT architecture are directly affecting the functionality of that layer. Authors in [11] reveal that in vital societal services, regardless of an overall optimistic view on IoT, security risks are neglected. Fig. 1 shows the architecture of IoT and it depicts how the four layers are using the different devices in IoT network for communication.

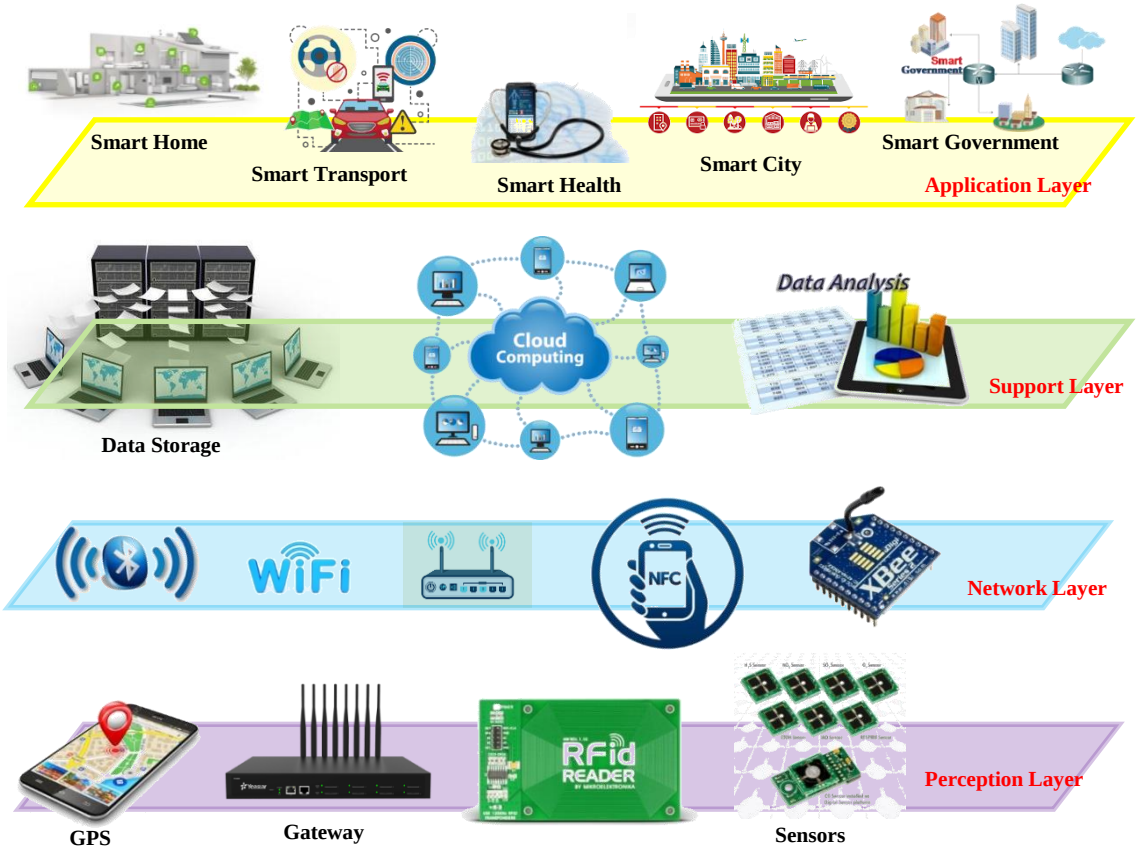

Fig. 1: IoT Architecture.

3.1. Perception layer

Perception layer is also known as Sensors layer which receives data from the environment through sensors. Sensors and RFID readers are used in perception layer and these have limited memory, low power, and limited computational ability that make it less secure. Sensors attached to devices capture the information from these participating devices. GPS is also used in this layer for location tracing for spatial applications over a network. In local and short-range communication, IoT node combination is done by the Perception layer. It observes, collects, processes and transmits data to the network layer. Threats in this layer majorly focus on data collection activities through sensors.

Threats to Perception Layer
There are various security risks related to perception layer. RFIDs, sensors and intelligent embedded technologies are vulnerable to several attacks in perception layer. Few security flaws and their possible risk mitigation solutions are mentioned here:

3.1.1. Secrecy and authentication

Outsider attacks like eavesdropping, replay attack, spoofing, and packet modification are some security risks on authentication and secrecy of the sensor network.
Protection
Good, efficient, robust and reliable cryptographic solutions can minimize these types of attacks.

3.1.2. Network availability

Attacks that effect the availability of the sensor network are generally referred as Denial of Services (DoS) attacks. As the sensor networks are divided into layers, so all the sensor network layers are vulnerable to this kind of DoS attack. A similar study of [12] gives Path-based DoS attack (PDoS) in which system availability is reduced and nodes batteries are exhausted.

3.1.3. Service integrity

In these types of attacks, an attacker makes the network to accept incorrect data values.
Protection
Cryptographic solutions minimize the attackers affect by not allowing them to decrypt the data.

3.1.4. Jamming

It is a DoS type attack in which the air-interface is affected by paralyzing the communication operations concerning reader and tag. Signal/ Radio jamming is such type of attack in which communication channel between nodes is occupied to obstruct their communication.
Protection
Early detection of jamming devices is a possible solution to avoid such attacks [9].

3.1.4. Eavesdropping

An attacker in this attack just monitors the communication among tag and the reader secretly to obtain the information. It's the wireless characteristics of RFID that an attacker sniffs out secret information like password and other confidential data. The tag data is mostly in plaintext form that makes this type of attack to occur [9].
Protection
Encrypting the data or limiting the distance between tag and reader is a possible solution for such attacks [9]. A similar study in [13] proposed an efficient random key agreement method which offers protection against eavesdropping attack in NFC.

3.1.5. Replay attack

Attacker interrupts communication between tag and reader and a duplicated tag is used in order to match the authentication sequences. This type of attack affects RFID tags and air-interface.
Protection

Data Encryption and tag authentication can minimize this attack [14]. A VLFSR function for lightweight encryption security which provides resistance against various attacks on RFID is proposed in [15]

3.1.6. Man-in-the-middle (MITM) attack

MITM attacks are also known as Relay attacks which are occurred during data transmission. Kfir and Wool give names to two communicating devices; these names are Leech and Ghost. A device placed close to the target RFID is named as Leech and the device placed closed to target reader is named as Ghost. Communication between these two devices i.e. Leech and Ghost creates an illusion of the connection that exists physically between the RFID device and the target reader.

Protection

Possible risk mitigation for such type of attack is using shielding, or short range tags or through the use of distance bounding protocols [16].

3.1.7. Blocking

When an attacker uses a blocker-tag so as to stimulate the presence of several tags and as a result, it causes Denial of Service (DoS). This happens because the reader is trying to inspect those non-existing tags. Air interface is affected by the blocking.

Protection

Detection of blocking devices early can minimize the effect of blocking [16].

3.1.8. Tag cloning

A duplicate tag is created by the attacker through illegitimate access which is based on the actual tag. It affects air-interface and RFID tags which results in the financial problems in applications.

Protection

To minimize this kind of attack, Tag authentication can be used. According to authors in [17], "Synchronized Secrets Method" by detecting cloning attacks provides a protection method for tag cloning. This method pinpoints the different tags which are having an identical ID.

3.1.9. Spoofing

In this attack, attackers broadcast a fake message to the sensor network by falsifying its originality and appearing as an original source. As a result, an attacker can obtain full access to the system [18].

3.1.10. Device tampering

Device Tempering is also known as Node-Capturing. In this attack, attacker replaces the sensor node by their malicious node as a result attaining total control over captured node [18].

3.1.11. Node outage

This attack blocks the functionality of network components like reading, collection, and initialization operations. It can be applied either logically or physically to the sensor network [19].

3.1.12. Information leakage

This attack is a passive leakage in which due to some accidental behavior a person gets an access to sensitive data to which no authorization is granted.

Protection

Authors in [17] proposed RFID-Tate, a lightweight protection method for protecting identity and Identity based Encryption (IBE) method for authentication. A similar approach of authors in [20] provides a conditional protection for privacy with less overhead.

3.2. Network layer

Data routing and communication among IoT hubs and other internet devices are the major tasks of the network layer. This layer is a central nervous system in IoT which is responsible for initial data processing and information broadcasting. This IoT layer uses modern wireless technologies like WiFi, Bluetooth, Zigbee, 3G, LTE etc. to run routing devices, gateways and switching. It is the network gateways that serve as the mediator between different IoT nodes. This is carried out by combining, filtering and communicating data between sensors in the network.

Threats to Network Layer

This layer deals with such attacks that can harm the availability of the network for communication among IoT devices. Related threats to network layer are listed below:

3.2.1. Selective forwarding

In such attacks, an attacker rather than forwarding all messages, selectively does not forward some messages and drop them. The malicious node forwards the remaining traffic to reveal its wrongdoing. A similar type of attack is given by authors in [21] which is called Neglect and Greed, where the subverted node skips routing some of the messages randomly.

3.2.2. Sybil attack

When an attacker is at more than one place at a time, as a single malicious node then it is called Sybil attack. In it, a malicious device is illegitimately holding several identities in the network. Such type of attacks affects the fault tolerant schemes [22].

Protection

Each node instances and spatial position of nodes can be observed by using Distributed Hash Tables [17].

3.2.3. Sinkhole / blackhole attack

Sinkhole or Blackhole attack is described by strong resource contention among nodes which are neighbors of the malicious node for limited channel access and limited bandwidth. As a result, there is congestion in the network and energy consumption of the nodes is increased.

When there is a sinkhole attack in sensor network then the network is also vulnerable to some other DoS attacks [23].

3.2.3. Wormhole

It is a kind of DoS attack in which Data bits in the network are relocated from its original position over a low-latency link [24].

Protection

A method to protect the authentication is proposed by the authors in [17], the proposed approach is "Markle tree authentication" method.

3.2.4. Man-in-the-middle (MITM) attack

In this MITM attack, communication between two parties is monitored and controlled by some unauthorized party hideously. This is accomplished by attaining the fake identity of the victim and then communicating to gain further information. It is also termed as a kind of eavesdropping attack [25].

3.2.5. Hello-flood attack

Introducing high traffic in the sensor network by congesting the channel with huge useless messages is known as Hello-Flood attack. In this attack, it is a malicious node that sends the useless message which is replied by the attacker thus, resulting in high traffic [26].

3.2.6. Acknowledgement flooding

Sensor-based systems frequently require routing algorithm to send acknowledgments. These acknowledgments are then used by a malicious node to send false information to destined neighboring nodes. It is a kind of Denial of Service attack [26].

3.3. Support layer

This layer is responsible for information collection, intelligent data processing and identifying the physical world. In mass data processing, handling malicious information smartly is very limited. According to the authors in [11], recognition of malicious information intelligently is not an easy task, it is a challenging job. Support layer is responsible for data storage activities, accessing cloud services for effective utilization of technologies over network and analysis of data to provide precise information.

Threats to Support Layer
Data storage technologies are mainly targeted by attackers in the support layer. Some most common attacks of this IoT application layer are discussed below:

3.3.1. Data tampering

This attack occurs when an inside person tampers the data either for self-benefits or for profit-making for some third-party.
Protection
Insider can easily make changes to the data so providing authentication to data is necessary to prevent from such attacks [27].

3.3.2. Unauthorized access

Attacker creeps into the system and may harm the sensitive data of the system. Attacks like, preventing access to related IoT services is one such type of attack.
Protection
Proper security mechanism should be provided to prevent the system from such attacks [28].

3.3.3. DoS attack

In this layer of IoT architecture, DoS attacks like system shut down that can harm the system or results in the unavailability of the system are possible effects of such attacks [27].

3.4. Application layer

This layer is responsible for providing services to all industries including Smart e-health, Smart transport, smart government, smart city etc. In application layer, the security requirement differs from application to application. One important characteristic of this layer is data sharing and this creates a problem for data privacy, authentication, integrity, confidentiality, access control, and information disclosure which are the security requirements of this layer [29]. In this layer of IoT architecture, the creation of a smart environment for applications is executed.

Threats to Application Layer
The application layer includes the tailored services that are as per user's interest and IoT applications. The responsibility of this layer is to provide the user interface to IoT devices [30]. Threats in this layer focus on the services provided by this layer, major threats applicable to this layer are mentioned below:

3.4.1. Sniffer/ logger

Sniffer/ Logger programs are introduced into the system by attackers to steal important information from the network traffic. An attacker may steal passwords, E-mail files, E-mail texts and other important information.

3.4.2. Injection

In this attack, a code is inserted into the application which is running on the server by an attacker. This results in data corruption or loss of data [31].

3.4.3. Session hijacking

Personal identities are revealed through this type of attack. This could be done by exploiting security flaws mainly in session management and authentication [31].

3.4.4. Distributed denial-of-service (DDoS)

DDoS is executed simultaneously by more than one attacker thereby leading to some Denial of Services in the network [25].

3.4.5. Social engineering

In this attack, information is retrieved via chats or by other social means by the attackers.
Protection
To minimize effects of such attacks, access to sensitive data should be provided to only authorized people. Policies for appropriate access management should be clearly defined along with assigning a physical identity.

4. Threats analysis

In IoT architecture, all the four layers are providing different functionalities and services with respect to the devices working for these layers. Each layer has different security threats particular to that layer requiring specific security solutions to be implemented. Authentication, authorization, integrity, confidentiality, data protection in sensor devices are some widely addressed security requirements in IoT environment.
Table 1 presents devices and services related to different IoT layers, various security threats to these layers and their respective security requirements.
If the above mentioned security requirements are not treated wisely in the smart environment, then these may result in security threats to the sensor networks. Authors in [32] presented a security architecture in which user's privacy is considered as a primary issue in the application layer and they considered security of information processing as an important aspect in support layer. Network layer is responsible for information communication in sensor networks, so security to information system is addressed by the network layer. Perception layer takes cares of security issues related to information collection.
Table 2 presents the description of various security risks which are also considered as security requirements in smart environment of IoT.
Analysis of security requirements in IoT provides a step forward in providing secure IoT environment. To deal with several problems resulting from threats in smart environment of IoT, this section presents direction and scope for future research. Integrity, authentication, confidentiality and digital signatures are major requirements in security. One of the most obvious and promising type of security solution is by providing efficient and good cryptographic algorithms which aims to fulfill major security requirements.
This paper is an attempt towards finding good security solutions by understanding various threats and security requirements in IoT enabled smart environment. Further, this paper also inspires researchers to work more on IoT security that might try to take a challenge that small memory and limited arithmetic operations are available in IoT.

Table 1: Devices and Services in IoT Layers with Major Security Threats and Their Possible Security Requirements

IoT Layers	Devices/ Services	Security Threats	Security Requirements
Application	Smart Home, Smart Environment, Smart City, Smart Health, Smart Government	Sniffers/ Loggers, Injection, Session Hijacking, DDoS, Social Engineering	Authentication, Integrity, Confidentiality, Access Control, Key Management, Data Management, Privacy Protection, Security Education
Support	Information Processing, Cloud Computing, Data Analysis, Data Storage	Tampering With Data, DoS Attack, Unauthorized Access	Secure Multiparty Computation, Secure Cloud Computing, Anti-Virus
Network	Communication Network (2G, 3G, 4G, 5G), Internet, Mobile Network, Routers, Bluetooth, Wi-Fi, NFC, ZigBee	Selective Forwarding, Sinkhole, Sybil Attack, MITM, Hello-Flood, Wormhole, Acknowledgement Flooding	Identity Authentication, Secure Network Access, Secure Data Communication
Perception	RFID Reader, Sensors, GPS	Spoofing, Signal/ Radio Jamming, PDoS, Node Outage, Eavesdropping, Replay Attack, Packet Modification, Tag Cloning, Device Tampering	Lightweight Cryptography, Sensor Data Protection, Key management

Table 2: Explanation of Various Security Risks in IoT

Risks/ Security Requirements	Explanation
Authentication	Defines if peers during negotiation are authenticated or not. In IoT, authentication of a server is required so as to assure clients about legitimate data. To achieve authentication unique shared key or PKC signature can be used[33].
Data Authentication	Information about the object and the address retrieved must be authenticated [32].
Integrity	Ensuring accuracy of data and providing un-tampered data to the users can be achieved by providing end-to-end security mechanism [34].
Confidentiality	Securely sending secret information of authorized personnel over network and not allowing data leakage to adjacent network.
Availability	Providing services to authorized personnel anytime from anywhere [35]. Critical IoT applications must be provided redundancy for IoT services and technologies.
Access Control	Access control must be implemented by the information providers on the provided data [32].
Key Management	Key must be kept secret from attackers so as to secure the data over network. Authors in [29] consider key management as an important aspect in lightweight cryptography.
Data Management	Cryptographic techniques and protocols along with specific designed data management policy is required for proper data management [36]
Privacy Protection	Providing customized tools for data management to the users is a way to achieve privacy protection [36].
Identity Authentication	Validating distinctive devices or users with authentication, authorization, accounting and provisioning ahead of allowing system usage to them is considered as an identity authentication[35].
Security Education	AS IoT includes national security, business secrets and individuals private information. So there is an urgent need to promote policies and regulations for IoT security which are neglected in present scenario[29].
Lightweight Cryptography	Being constrained with a number of new factors, there a need to develop and implement lightweight ciphers and ultra-lightweight ciphers for wireless sensor networks in IoT.
Sensor Data Protection	Only information providers should be allowed to infer the customer information [32].
Secure Storage	Sensitive information in the system must be stored with confidentiality and integrity [35].
Identity Authorization	Identifying objects in the sensor networks by associating user rights and restrictions is considered as an identity authorization [35].
Secure Data Communication	Confidential communication among peers must be authenticated ensuring data integrity and identity protection of sensor objects [35].
Secure Network Access.	Connection and services would be provided only after the authorization of devices [35].
Secure Cloud Computing	Critical IoT applications using cloud services require security and privacy. Providing tags identity and addressing to the objects in IoT provides support for cloud computation in sensor networks [37].
Secure Multiparty Computation	Providing privacy-preserving techniques for data mining can be provided by secure multiparty computation [38].

5. Conclusion

IoT is rapidly finding its path in the modern IT arena. The main aim is to improve the quality of life by providing several smart applications. This paper presents an overview of new enabling technologies contributing to IoT for successful implementation. Further, some issues and challenges pertaining to the deployment of IoT architecture have been presented. In IoT architecture, functionality of each layer is explained with respect to the devices working on it and services it provides. There are security issues related to each layer and these issues should be dealt with by providing some proper security mechanism. Risk classification provides an opportunity to direct the research work in proper direction. Layers most vulnerable to threats can be provided more attention. This paper presents various security threats related to each of the IoT layer and security requirements as imposed by these layers. Feasible ways to provide solutions to these security requirements are also presented in this paper. This paper provides insights into new challenges that a smart environment is facing with the deployment of IoT.

References

[1] Razzak, F., Spamming the Internet of Things: A Possibility and its probable Solution, *Procedia computer science*, vol. 10 (2012) 658-665. https://doi.org/10.1016/j.procs.2012.06.084.

[2] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., Internet of Things (IoT): A vision, architectural elements, and future directions, *Future generation computer systems*, vol. 29, no. 7 (2013) 1645-1660. https://doi.org/10.1016/j.future.2013.01.010.

[3] Kumar, J.S. and Patel, D.R., A survey on internet of things: Security and privacy issues, *International Journal of Computer Applications*, vol. 90, no. 11 (2014).

[4] Bertino, E., Data Security and Privacy in the IoT, *Proc. 19th Int. Conf. Extending Database Technol.*, (2016) 1-3.

[5] Qiang, C., Quan, G.R., Yu, B. and Yang, L., Research on security issues of the internet of things, *International Journal of Future Generation Communication and Networking*, vol. 6, no. 6 (2013) 1-10. http://www.earticle.net/Article.aspx?sn=217332 https://doi.org/10.14257/ijfgcn.2013.6.6.01.

[6] Khan, R., Khan, S.U., Zaheer, R. and Khan, S., Future internet: the internet of things architecture, possible applications and key challenges, *10th International Conference on Frontiers of Information Technology (FIT)*, (2012) 257-260. IEEE. https://doi.org/10.1109/FIT.2012.53.

[7] Sarkar, C., Nambi, S.A.U., Prasad, R.V. and Rahim, A., A scalable distributed architecture towards unifying IoT applications, *World Forum Internet of Things (WF-IoT)*, (2014) 508-513. IEEE. https://doi.org/10.1109/WF-IoT.2014.6803220.

[8] Ungurean, I., Gaitan, N.C. and Gaitan, V.G., An IoT architecture for things from industrial environment, *10th International Conference on Communications (COMM)*,(2014) 1-4. IEEE. https://doi.org/10.1109/ICComm.2014.6866713.

[9] Kulkarni, G., Sutar, R. and Mohite, S., RFID security issues & challenges, *International Conference on Electronics and Communication Systems (ICECS)*, (2014) 1-4. IEEE. https://doi.org/10.1109/ECS.2014.6892730.

[10] Chen, X.Y. and Jin, Z.G., Research on key technology and applications for internet of things, *Physics Procedia*, vol. 33 (2012) 561-566. https://doi.org/10.1016/j.phpro.2012.05.104.

[11] Asplund, M. and Nadjm-Tehrani, S., Attitudes and perceptions of IoT security in critical societal services, *IEEE Access*, vol. 4 (2016) 2130-2138. https://doi.org/10.1109/ACCESS.2016.2560919.

[12] Deng, J., Han, R. and Mishra, S., Defending against path-based DoS attacks in wireless sensor networks, *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* (2005) 89-96. ACM. https://doi.org/10.1145/1102219.1102235.

[13] Jin, R., Du, X., Deng, Z., Zeng, K. and Xu, J., Practical secret key agreement for full-duplex near field communications, *Transactions on Mobile Computing*, vol. 15, no. 4 (2016) 938-951. IEEE. https://doi.org/10.1109/ACCESS.2016.2560919.

[14] Khoo, B., RFID as an Enabler of the Internet of Things: Issues of Security and Privacy, *Internet of Things (iThings/CPSCom), 4th International Conference on Cyber, Physical and Social Computing* (2011) 709-712. IEEE. https://doi.org/10.1109/iThings/CPSCom.2011.83.

[15] Garcia-Alfaro, J., Herrera-Joancomarti, J. and Melia-Segui, J., Security and privacy concerns about the RFID layer of EPC Gen2 networks, *Advanced research in data privacy*(2015) 303-324. Springer, Cham. https://doi.org/10.1007/978-3-319-09885-2_17.

[16] Kfir, Z. and Wool, A., Picking virtual pockets using relay attacks on contactless smartcard, *Proc. - First Int. Conf. Security and Privacy for Emerging Areas in Communications Networks*(2005) 47-58. IEEE. https://doi.org/10.1109/SECURECOMM.2005.32.

[17] Cvitić, I., Vujić, M. and Husnjak, S., Classification of security risks in the IoT environment, *26th Daaam International Symposium on Intelligent Manufacturing and Automation* (2016) 0731-0740.

[18] Mitrokotsa, A., Rieback, M.R. and Tanenbaum, A.S., Classifying RFID attacks and defenses, *Information Systems Frontiers*, vol. 12, no. 5 (2010) 491-505. https://doi.org/10.1007/s10796-009-9210-z.

[19] Anwar, R.W., Bakhtiari, M., Zainal, A., Abdullah, A.H. and Qureshi, K.N., Security issues and attacks in wireless sensor network, *World Applied Sciences Journal*, vol. 30, no. 10 (2014) 1224-1227.

[20] Eun, H., Lee, H. and Oh, H., Conditional privacy preserving security protocol for NFC applications, *Transactions on Consumer Electronics*, vol. 59, no. 1 (2013) 153-160. IEEE. https://doi.org/10.1109/TCE.2013.6490254.

[21] Sharma, P., Saluja, M. and Saluja, K.K., A review of selective forwarding attacks in wireless sensor networks, *International Journal of Advanced Smart Sensor Network Systems*, vol. 2, no. 3 (2012) 37-42. https://doi.org/10.5121/ijassn.2012.2304.

[22] Pooja, M. and Singh, D.Y., Security issues and sybil attack in wireless sensor networks, *International Journal of P2P Network Trends and Technology*, vol. 3, no. 1 (2013) 7-13.

[23] Ahmed, N., Kanhere, S.S. and Jha, S., The holes problem in wireless sensor networks: a survey, *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 2 (2005) 4-18. https://doi.org/10.1145/1072989.1072992.

[24] Karlof, C. and Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, *Ad hoc networks*, vol. 1, no. 2-3 (2003) 293-315. https://doi.org/10.1016/S1570-8705(03)00008-8.

[25] Farooq, M.U., Waseem, M., Khairi, A. and Mazhar, S., A critical analysis on the security concerns of internet of things (IoT), *International Journal of Computer Applications*, vol. 111, no. 7 (2015) 1–6.

[26] Borgohain, T., Kumar, U. and Sanyal, S., Survey of security and privacy issues of Internet of Things. *arXiv preprint arXiv:1501.02211*. (2015).

[27] Shi, E. and Perrig, A., Designing secure sensor networks, *IEEE Wireless Communications*, vol. 11, no. 6 (2004) 38-43. https://doi.org/10.1109/MWC.2004.1368895.

[28] Tyagi, S., Darwish, A. and Khan, M.Y., Managing computing infrastructure for IoT data, A*dvances in Internet of Things*, vol. 4, no. 3 (2014) 29–35. https://doi.org/10.4236/ait.2014.43005.

[29] Suo, H., Wan, J., Zou, C. and Liu, J., Security in the internet of things: a review, *International Conference on Computer Science and Electronics Engineering (ICCSEE)*, vol. 3 (2012) 648-651. IEEE. https://doi.org/10.1109/ICCSEE.2012.373.

[30] Leloglu, E., A review of security concerns in Internet of Things, *Journal of Computer and Communications*, vol. 5, no.1 (2016) 121-136. https://doi.org/10.4236/jcc.2017.51010.

[31] Autili, M., Inverardi, P., Tivoli, M. and Garlan, D., Synthesis of correct adaptors for protocol enhancement in component-based systems, *Specif. Verif. Component-Based Syst.* (2004).

[32] Weber, R.H., Internet of Things–New security and privacy challenges, *Computer law & security review*, vol. 26, no.1 (2010) 23-30. https://doi.org/10.1016/j.clsr.2009.11.008.

[33] Roman, R., Alcaraz, C., Lopez, J. and Sklavos, N., Key management systems for sensor networks in the context of the Internet of Things, *Computers & Electrical Engineering*, vol. 37, no. 2 (2011) 147-159. https://doi.org/10.1016/j.compeleceng.2011.01.009.

[34] Yousuf, T., Mahmoud, R., Aloul, F. and Zualkernan, I., Internet of Things (IoT) Security: Current status, challenges and countermeasures, *International Journal for Information Security Research*, vol. 5, no. 4 (2015) 608-616. https://doi.org/10.20533/ijisr.2042.4639.2015.0070.

[35] Babar, S., Mahalle, P., Stango, A., Prasad, N. and Prasad, R., Proposed security model and threat taxonomy for the Internet of Things (IoT), *International Conference on Network Security and Applications* (2010) 420-429. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14478-3_42.

[36] Pescatore, J. and Shpantzer, G., Securing the internet of things survey, *SANS Institute* (2014) 1-22.

[37] Botta, A., De Donato, W., Persico, V. and Pescapé, A., Integration of cloud computing and internet of things: a survey, *Future Generation Computer Systems*, vol. 56 (2016) 684-700. https://doi.org/10.1016/j.future.2015.09.021.

[38] Lindell, Y. and Pinkas, B., Secure multiparty computation for privacy-preserving data mining, *Journal of Privacy and Confidentiality*, vol. 1, no. 1 (2009) 59-98. https://doi.org/10.29012/jpc.v1i1.566.