International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I6P219

Volume 70 Issue 6, 155-164, June 2022

Research Article

Remediation Measures to Make the Insecure Internet of Things Deployment Secure

Srabana Pramanik[1], Deepak. S. Sakkari[2] and Sudip Pramanik[3]

[1,2] *Department of Computer Science & Engineering, Presidency University, Bangalore-560064, India*
[3]*DXC Technology, Bangalore-560035, India*

[1*]srabana.edu@gmail.com

Received: 04 April 2022 Revised: 19 May 2022 Accepted: 02 June 2022 Published: 27 June 2022

Abstract *- In the globalized era, daily activities largely depend on smart services like E-marketing, Smart health care, E-farming, Smart home, Smart waste management, Smart emergency services, etc. Most activities become smarter with the Internet of Things (IoT) support. Day by day, the diapason of the IoT application sphere increases exponentially. This flourishment of IoT brings lots of security issues. Because the Internet of things is a resource constraint device, it has limited resources like minimum storage capacity, less battery backup, limited speed of processing, etc. in these phenomena, the conventional security filter will not perform. to hold the security aspect of IoT tightly, there is a need for a very lightweight encryption technique, authentication technique, and a modified architectural framework. in this paper, the existing architectures, threats, and vulnerabilities of IoT are studied and analyzed. Along with that, the recent empirical review of remediation security measures on IoT deployment is discussed. Furthermore, a security architecture has been proposed as a countermeasure to enhance the security of the IoT deployment, and a combined protocol stack is elaborated.*

Keywords *- Attacks on IoT, Internet of things (IoT), Security threat, Vulnerability.*

1. Introduction

According to the ITU (International Telecommunication Union), the Internet of Things (IoT) is defined as a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies [1]. in today's world, the dependency on IoT devices is increasing day by day.

In 1980 RFID was the fundamental technology for IoT. the attached RFID tag chip transmits its identity value to an RFID reader to track, maintain, and monitor the objects through wireless communication. During this period, RFID was used in logistics, supply chain management, retailing, etc. [2]. Later in 1990 Wireless communication network came, which used intelligent connected sensors to collect the environment's raw data and monitor the system. Monitoring Applications of WSN are Healthcare Monitoring, Traffic monitoring, etc. [3],[4]. in 1999 Kevin Ashton first introduced the Internet of Things (IoT) as an object of the global network while explaining a supply chain application where IoT devices were connected with RFID [5].

Afterward, the journey of IoT started with the advancement of technology from smart home to industry, agriculture to animal farming, transport to connected healthcare, smart retail application to supply chain management, smart wearables to the smart security system, etc.

As the number of domains increases, security threats are also increasing exponentially. All IoT devices are resource-limited and operated in open spaces where security is very low. This situation always invokes the intruder to do malicious activity on them.

To make the IoT deployment secure, it is required to tight three areas: 1) Secure data communication over the IoT environment, 2) adopt an efficient authentication technique that can authenticate the legitimate parties for further communication and secure the system from various attacks, 3) design a secure system architecture and protocol stack which can protect the IoT ecosystem from various hazards. in this paper, the main focus is on the third category.

The Contributions of the paper are as follows:

- Discussing the components of IoT and giving light on the basic layered architecture and communication structure of IoT application (Section II)
- Elaborating the upcoming security threats & vulnerabilities associated with the IoT environment (Section III).
- Empirical review of countermeasures to enhance the IoT deployment (Section IV).

- Proposed a generic ten-layered architecture which can be an improvised version of the existing basic architecture to enhance the security of the IoT applications, and a combined secure protocol stack is elaborated (Section V).

2. All about the Internet of Things

2.1. Elements of IoT

The device should contain the following elements to offer the Internet of Things functionality.

2.1.1. Identification

A device or object can be identified within a network. Identification can be possible in two ways i) naming and ii) addressing. Electron product codes (EPC) and ubiquitous codes are utilized to offer the name of an object in a specific network [6]. IPv4 and IPv6 are used to give a unique address to the particular device. IPv6 uses 128-bit address space. It can address the upcoming demand.

2.1.2. Sensing & Actuating

The IoT end-node devices are implanted with sensors and actuators. A sensor senses the real-time information from the environment and sends the same data to the cloud for further processing. After analysis, if any control information comes, the actuator will follow that command and perform the specific action.

2.1.3. Communication

Communication is the essential activity of IoT. Various techniques are used to communicate the data inside the IoT environment. Radio Frequency Identification (RFID), Bluetooth, Long-Term Evolution (LTE), Near Field Communication (NFC), WiFi, etc., techniques facilitate the communication in IoT deployment [7],[8].

2.1.4. Computation

After data collection, various computation operations are performed on the collected data. They are removing unnecessary information, cleaning, filtering the data, etc. All kinds of computations are performed at the hardware level by Arduino, Raspberry Pi, and Intel Galileo or at the software level with the help of various IoT operating systems such as TinyOS, Android, LiteOS etc.[9].

2.1.5. Services

Generally, the Internet of Things provides five categories of services. the first one is Identity services which either provide the object's identity or identify from which identity source the request has come. the second is the Aggregation service which collects information from several objects and processes them. Third is collective services which take the decision from the result of data analysis and send an appropriate request to the specific device based on the result. the last is ubiquitous service which takes action without observing the surrounding.

2.1.6. Semantics

It behaves like the brain of the system. It performs the ultimate responsibility to satisfy the end-user demand. Based on the collected data, take the decision and sends proper responses to the customers.

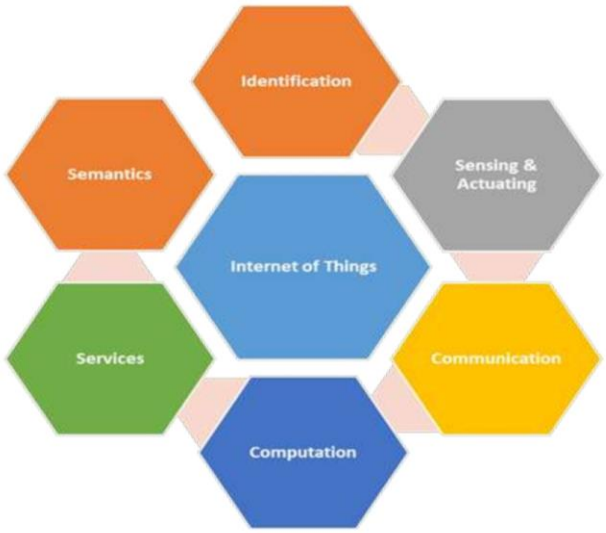

Fig 1. (Color online) Elements of IoT

2.2 Basic IoT Architecture used by different applications

2.2.1. IoT Architecture

There is no standard architecture for the IoT environment which is recognized globally. the different researcher has presented various application-specific multi-layers of architecture for IoT deployment. the architecture layer depends on technology, business technical requirements, and needs.

The basic architecture has three layers [10].

1) The perception layer or sensor layer is a physical layer or recognition layer. the main components of this layer are sensor that collects information, including environmental condition and properties of objects, and identifies and control the world. It is used as a bridge between the real world and the digital world.

2) The network layer: the main role is to connect all the smart things, network devices, and networked servers under one umbrella so that they can share information. It provides faithful data transmission after initial processing, classification, and polymerization. the network layer is called the Central Nervous System, which provides worldwide services of IoT.

3) The application layer is the Outer-most layer which affords personalized services to the end-users. Users can access these physical things or the internet of things

remotely through some application with the help of mobile devices.

The International Telecommunication Union states that the IoT architecture must have five layers. They are the sensing layer, accessing layer, networking layer, middleware layer, and application layer. Yang et al. [11] proposed the IoT system architecture with four layers. It includes one extra layer that is support layer. It analyzes, processes, and stores a large amount of data from down layers. the support layer provides security features to IoT architecture. This layer checks whether the information is coming from an authenticated user or not and transmits the verified data to the network layer. Here the medium of transmission is either wireless or wired.

Some researchers proposed five-layered architecture, which includes extra processing and semantic layers [12] to add extra features to the system.

The processing layer is alternatively known as the middleware layer. It also analyzes, processes, and stores a large amount of data from the network layer. the layer removes the extra information, extracts the original data from that, and helps solve the big data problem of IoT.

The semantic layer is also called a business management layer. This layer uses various technologies to offer essential services to the end-users, such as data mining, business intelligence, visualization, analysis, and decision-making. It helps in sales activities /support work.

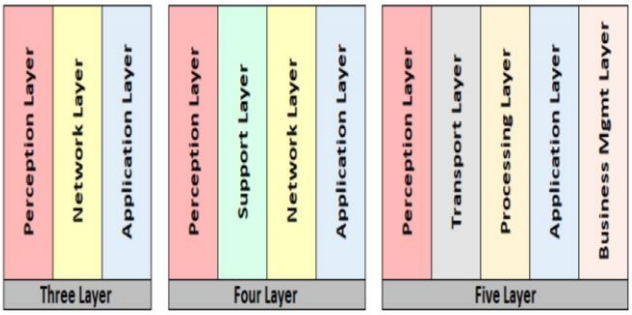

Fig 2. (Color online) Different layered architectures of IoT

Based on requirements, the different researcher focuses on a different layered architecture.

2.3. IoT Communication structure

(Figure 3) describe the communication structure of IoT. the IoT communication network has a two-part local network/ subnetwork and a global network. It contains mainly physical objects or things, and Edge routers, gateways, Cloud servers, IoT services, and device controllers [13].

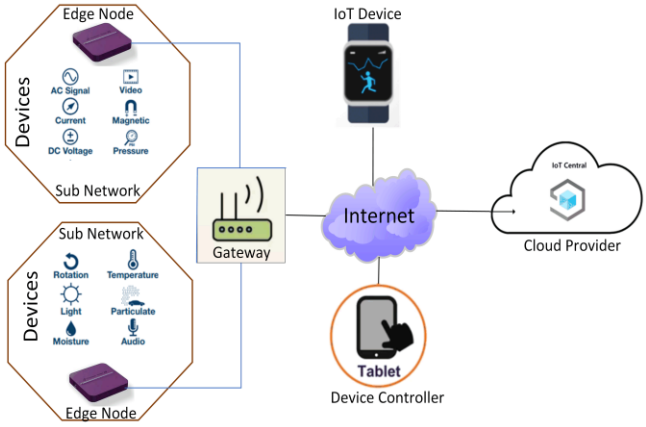

Fig 3. (Color online) Communication IoT infrastructure

The Low power Things or devices are embedded with sensors, actuators, communication interfaces, operating systems, and other services. Sensors collect data from the environment, and the actuator also takes necessary action and shares the information with other devices.

Edge Nodes or Coordinators are used to connect devices to a gateway. One or more devices can be connected with an Edge node. It collects data from them and routed the packets to a proper channel through one or more edge nodes or a gateway node. It does analysis and few preprocessing works before sending to deeper data mining intelligence. the main duty of an edge node is to monitor the devices, send a summary of the periodical activity of actions, and provide events to the IoT service provider.

Gateways Node is a multiprotocol device. This device works like a bridge between the local networks and the cloud. It provides routing infrastructure between device subnetworks and things to a cloud server. It is responsible for identifying the valuable data from the huge amount of raw data collected from sensors. the gateway performs local analytics and sends the result to the data center or cloud. If required, it sends the analytics to edge devices to control the environment condition.

IoT services is a software application hosted in the cloud so that all Users can access the IoT devices remotely. This service provides Process automation, device management, and decision making.

Cloud Servers: IoT system gets huge shared data storage, processed data, and processing power from the cloud. in all IoT applications, there is the two-part one collecting data and developing some mitigating action to control the situation. the second part is initiated in the cloud after performing lots of analytics to get useful information.

Device controller, with the help of these devices, the user can issue commands for different IoT applications. in

smart parking, a user can access the application through smart mobile or tablet.

3. Security Threats & Vulnerabilities of IoT

Today everybody knows that IoT is a proactive, scalable worldwide network infrastructure where all network devices and things have virtual representation and are connected to the internet and with each other and provide intelligent integrated communication services. It is a growing network where the no of devices grows exponentially. A few years ago, only a few areas like meter reading, greenhouse monitoring, telemedicine monitoring, and transport system were getting intelligence from IoT [14]. Now almost every sector offers interconnection of things and provides global communication through the internet. Due to this, the entire IoT ecosystem comes under the threat of security in terms of privacy, unauthorized access, and more. Which brings lots of challenges and threats to security in terms of privacy, unauthorized access, and more

3.1. Security Threats

The main security threats in the IoT sector are:

3.1.1. Confidentiality

Unauthorized access of a user's confidential data is called the invasion of user privacy, which threatens Confidentiality [15].

3.1.2. Integrity

When data is transmitted through a public channel, it may be changed by the intruder or the malicious users or by the improper channel properties like electromagnetic disturbances. All of this threatens the integrity of data [16].

3.1.3. Availability

Denial of Service attack or DoS attack and Sinkhole attack control the natural flow of data, block the information available to the end-user, and create an Availability threat [17].

3.1.4. Authenticity

It is related to the Authentication threat. Unauthorized access to confidential data can destroy the integrity of personal information. Authenticity is very much important

3.1.5. Non-Repudiation

In an IoT environment, non-Repudiation means trustful communication, which can be under threat when there will be loss of connection, improper medium, constrained resources, etc. [18].

These security requirements are very important to provide end-to-end protection for IoT paradigms.

3.2. Vulnerabilities of the Internet of Things

IoT devices are always vulnerable to threats due to their limitation of power and constraint memory capacity. According to research analysis of IoT security, IoT Vulnerabilities are classified into nine types [19].

3.2.1. Lack of Physical security

Most IoT end-node devices work in an open environment, where anybody can do any malicious activity on them. They can get unauthorized access to them. and may damage the device physically and modify the cyber data by using some schemes [20],[21].

3.2.2. Inadequate Energy Harvesting

By characteristically, IoT devices are energy constraints. They cannot rejuvenate the energy automatically. An attacker may try to evacuate the energy by sending lots of fake messages and making the system down [22],[23].

3.2.3. Improper Authentication

Inefficient authentication strategy leads to various spiteful activities. It spoils data integrity, Confidentiality, and availability [24], [25].

3.2.4. Excess open ports

Most IoT devices are used as input devices. It will sense the environment condition and collect real-time data. But the main disadvantage is that all the devices have some unnecessary open ports, which invite the attacker to create some malicious activity [19].

3.2.5. Inefficient Encryption of data

Proper encryption techniques provide data protection and data transmission security so that an authorized user can only access it. If an attacker breaks the cryptosystem, they will get access to the system [26].

3.2.6. Improper Auditing mechanism

Some Security auditing frameworks ensure the security of IoT devices. But there is no proper auditing framework that can audit the three components of vulnerabilities combinedly: i) communication of IoT devices, ii) hardware, and iii) software/firmware. Some commercial tools are the Shodan API, which filters the connected devices to the internet, and IoTSploit, which does vulnerability checking and firmware analysis. Barbara provides consultation to IoT devices about a software security threat.[27]-[28],

3.2.7. Weak access control

Lack of user knowledge makes the system vulnerable. Most of the time, IoT devices use less complex passwords. the installation users are not instructed to change the login credentials. Hence attackers gain access to the entire system [28].

3.2.8. Not proper programming practices

Due to this, many attackers get unauthorized access to the system. Do the information modification [29].

3.2.9. Lack of proper patch management capabilities

Most IoT systems do not provide security patches in a particular time interval. Sometimes they don’t have an

automated patch updating facility also, and if it is available, it can't guarantee data integrity [29].

4. Empirical study of Countermeasures against security threats on IoT

This section gives an overview of empirical analysis of related research papers on security, privacy, and solution to tackle different threats to the IoT paradigm.

Keoh et al. [30] reviewed the standardization of security solutions for IoT infrastructure. They gave an overview of the efforts of the Internet Engineering Task Force (IETF) toward standardization. the interoperability of IoT devices will work properly when standardized communication security is there. in the end, they discuss some standardization techniques that can work with CoAP (Constrained Application Protocol) and enrich the Datagram Transport Layer security protocol.

Krishnaraj and Sangeetha [31] explained data privacy preserving techniques for the IoT environment. Various cryptographic techniques and privacy management processes are elaborated with present threats and vulnerabilities.

Pongle et al. [32] developed an intrusion detection system in different works. It can detect the Wormhole attack and attacker. the system first uses the location details of the node and its neighboring information to detect the attack and then identifies the attacker node by signal strength. the proposed scheme is very energy efficient.

Further, Mahmood et al. [33] presented a lightweight authentication protocol for the SmartGrid environment using the hybrid Diffle-Hellman technique, which includes AES and RSA for session key generation, and took advantage of the HMAC technique. in a Smart grid, all smart homes are equipped with a smart meter that records the customer's consumption details and sends the information to the service provider. Some access controlling technique is essential to protect this smart device from unauthorized access. This scheme provides authentication and protection against Man-in-the-Middle attacks and replays attacks. the proposed technique reduces the communication cost and computation overhead in the handshaking process by 20% to 30%.

H et al. [34] developed a new security model for the RFID system, which protects against attacks through a proper authentication scheme, including Quantum key distribution. Optical fibers distribute the quantum keys among RFID tags, readers, and EPC servers and provide authentication between them.

Tewari et al. [35] also proposed a lightweight authentication technique for tagged IoT things in a similar domain. It provides secure communication through insecure mediums and protects them from attacks such as DDOS, Tracking, Replay, etc. the proposed scheme uses only bitwise operation twice, providing another level of security from Tango attacks.

Stephen et al. [36] presented an Intrusion-Detection-System (IDS) that can identify the sinkhole attack. It uses detection metrics to record all outgoing and incoming packets and provides an Intrusion Ratio (IR). This IR value helps to find out whether a router node is malicious or not. IDS system sends the alert information to the leaf nodes.

Lin et al. [37] elaborated a new concept. He showed two kinds of communication models in the IoT world. One where the user can directly connect with an authentication server and another one where the user can connect with a special device instead of a gateway server. They proposed an integrated authentication technique that can protect against most attacks such as password guessing attacks, impersonation attacks, replay attacks, etc.

Further, Faurkanet et al. [38] developed a Deep learning-based approach to find the routing attacks on Big data. Here the proposed model can detect Decreased rank attacks, version number attacks, and Hello-Flood attacks which are coming under routing attacks. in this article, they have used the Cooja IoT simulator to develop an attack dataset. the attack dataset (IRAD) has 64.2 million values. the proposed model trained with the dataset and showed a scale-up performance.

The study by M.A Uddin et al. [39] designed a continuous Remote Patient Monitoring infrastructure. Here Patient-Centric Agent (PCA) is the central part of the system. PCA uses blockchain to store patient data to maintain privacy, share information among healthcare professionals, and integrate electronic health records through real-time patient monitoring. PCA maintains more than one blockchain for the same patient, reducing energy consumption while modifying the prefix tree blockchain.

Again, Gang Lin et al. [40] proposed a new concept. They designed a game model which analyze the attack benefits between the attacker/intruder and the defender. to help the defender, they proposed an enhanced-distributed-low-rate attack-mitigating (eDLAM) mechanism. It uses a lightweight malicious-request-table (MRT) and forwarding-state-table (FST). Here an optimal threshold updatation method is used by eDLAM, which provides maximum defender utility. in the end, the eDLAM is evaluated with the help of a false-negative rate and false positive rate and provides enhanced performance.

The study conducted by Dammak et al. [41] proposed a lightweight Authentication technique, TBLUA (Token-Based Lightweight User Authentication), to secure the access control between the user and smart devices through the Reservation Server and Registration Authority for a particular interval of time. Here they had used lightweight

XOR and hashed function, which enhanced the performance analysis compared to others.

Alternatively, Mostafa et al. [42] proposed an authentication procedure to authenticate the IoT end-node devices and the authentication server. Not only that, it established a private session key agreement too. They have used Physical Unclonable Functions and Hashing algorithms for this purpose. the proposed scheme scales up concerning memory storage, energy consumption, communication overhead, and computation complexity.

Ambarkar and Shekokar [43] proposed an authentication technique that can block the unauthenticated node to protect the IoT infrastructure from numerous attacks. the technique is tested against attacks like hello flood attacks, version number attacks, rank attacks, etc.

The important security requirements are collected from ten IoT applications during the security requirement analysis. It is observed that among ten applications, except SmartGrid, all applications need proper authentication, data availability, and services as an important security requirement. Figure 4 shows the fact clearly.

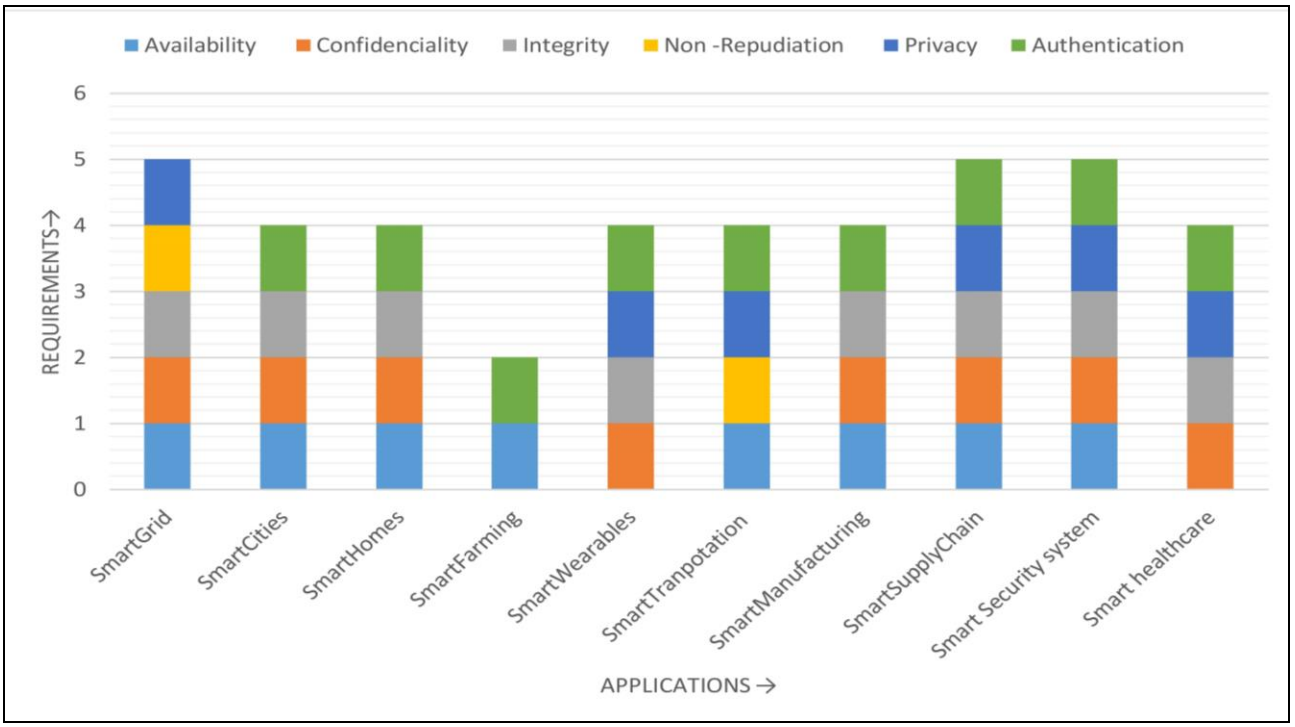

Fig 4. (Color online) Security requirement of IoT Applications

According to Ning and Wang's [44]'s proposed architecture, the entire work follows the human brain mechanism. the reference architecture had three parts. Every part worked according to the human brain organs.

Bonomi et al. [45] proposed a layer-based Fog architecture that had a few extra layers, such as monitoring, storing, and pre-processing layers as extra layers along with the basic three-layered architecture. These extra layers brought additional features to the proposed system.

The study conducted on IoT architecture by Burhan et al. [46] demonstrated the recent security issues of IoT layers. to overcome that, they designed a six-layered reference architecture to fight against upcoming threats.

A recent study by Pena and Fernandez [47] explained a new architectural model for cloud IoT platforms based on the blockchain concept, which provides a security safeguard from upcoming attacks.

Many researchers take various security measures to enhance and rectify security flaws. An improvised architectural model is elaborated in the following section, which can resolve most of the security flaws.

5. The Proposed Security architecture and Protocol stack

5.1. Proposed Architecture

After an in-depth analysis, a Layered security architecture (IoT) is proposed, which can protect the IoT infrastructure from many attacks. It has 10 layers. Following are the ten layers of architecture. (in Figure 5).

5.1.1. Device layer or Perception layer

This layer contains physical sensors and actuators to collect the environment's real-time data and convert them into digital format before sending them to the upper layer. If the data exceeds a threshold value, then after getting a response from the upper layer, the actuator can perform some specific action also.

5.1.2. Tracking layer

This layer is known as the monitoring layer. It will observe and checks the identity of all objects. After collecting the information from the sensor, the layer will verify whether the data is corrupted or not. Then it will pass the data to the next level.

5.1.3. Pre-processing layer

The initial processing is done through Filtering and analyzing the sensor data.

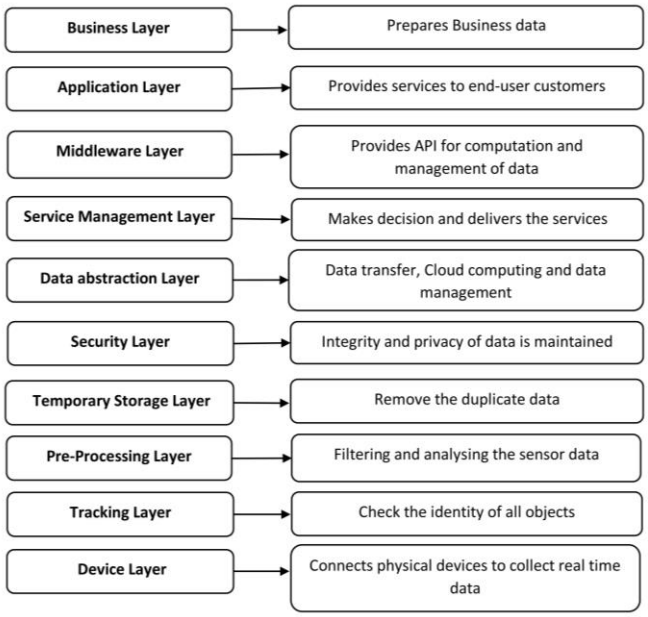

Fig 5. Proposed 10 layers of Security Architecture

5.1.4. Temporary Storage layer

Removes the duplicate data and maintains the temporary storage.

5.1.5. Security layer

Before sending the data to the data abstraction layer, the present layer maintains the security and fixes the integrity and privacy of data through proper Encryption/decryption.

5.1.6. Data abstraction layer

Transfer the data of the object layer through different technologies like ZigBee, Bluetooth low energy, infrared, GSM, WiFi, etc. Cloud computing and data managing works are also performed in the presentation layer.

5.1.7. Service Management layer

This layer pairs the requester's name and address with the required service. It processes the data sent by the Data abstraction layer, makes the decision, and delivers the service over the network.

5.1.8. Middleware layer

This layer hides the heterogeneous details of smart things in the application layer and makes a bridge between them. It provides the application Programming Interface (API) for computation and data management. This layer increases the interoperability of things and offers services to the end-users. Many open-source solutions exist in the market: OpenIoT, Middleware, Hydra, FiWare, etc. [48]-[51].

5.1.9. Application layer

Provides high-quality smart services to the customer based on their requirement. For example, an in-vehicle management system can send the acceleration and motion of a vehicle when asked for it.

5.1.10. Business Layer

This layer maintains all IoT infrastructure activities related to the entire system's application and business. It prepares a Business Model or develops some graphs or flowcharts constructed from the Application layer's data.

5.2. Proposed IoT protocol stack for the security establishment

The secure protocol stack of IoT is shown here (in Table 1), encountered during the literature survey.

The physical layer contains the IoT objects. the main duty of this layer is to maintain connectivity among all the devices or objects. Physical networks connect them with other objects or networks. Some popular protocols of these layers are Ethernet, RFID tags, Rj-45, PLC, ODB2, IEEE 802.15.4e, etc. A few popular protocols, EEE 802.15.4e and ZigBee, are generally used for personal area networks, local area networks, and home area networks. RFID-based protocols are also there, which include RFID, DASH7, NFC, etc.

Network Layer uses different protocols for different services, and they are IPv6, WirelessHART, RPL, NFC, RFID, GSM, 6LowPAN, LoRaWAN, SIGFIX, BB-IoT, etc. Data Packets are addressed and routed appropriately through the network layer.

The transport layer uses TCP/UDP, DTLS, TLS, QUICC DTLS, etc., protocols for end-to-end security and data transmission.

The application layer provides data formatting and presentation. But before that, it establishes a session. This

layer uses CoAP, MQTT, XMPP, AMQP, REST, etc. Protocols.

The last layer, that's Semantic layer, also uses different types of protocols for different services. For data aggregation, they may use MapReduce, Plume, etc. They may use Hadoop and MongoDB for data storing and retrieving. Overall, every kind of activity is maintained by this layer.

Table 1. (Color online) IoT security protocol stack

Layers	Protocols Used	Services
Semantic Layer	MapReduce, RapidMQ, Plume	Aggregation
	Hadoop, Hbase, MongoDB	Storing or retrieving
Application Layer	CoAP, MQTT, AMQP, DDS, XMPP	Session Establishment
Transport Layer	UDP, TCP, TLS, DTLS, QUIC, DTLS	End to End secure Communication
Network Layer	IPv6, 6LoWPAN	Addressing
	WirelessHART, RPL, NFC, RFID, GSM, Z-WAVE, WiFi	Short Communication
	LoRaWAN, SIGFOX, BB-IoT, WeightLess	Long Communication
Physical Layer	IEEE802.15.4e, RFID Tags, PLC, Rj-45, ODB2	Connections

Table 2. Details of important Communication protocol

Type of Protocol	Protocols for Communication	Advantage	Disadvantage
Sensor-Specific-Network protocols	RPL	Slow Processing power	Many attacks prone
	NFC	Simple structurer	Work on the limited area
	Bluetooth	Less consumption	Identity can be tracked
	Zigbee	Less consumption & low-cost devices are used	Transmission of a key is difficult
	WiMax	Use the proper authentication method	Mobility in a limited area
	WiFi	Efficient & mobile in nature	Reachability is very limited
Gateway-specific-network protocols	6LoWPAN	Slow Processing power	Lack of Authentication support
	3G/4G/5G	portability	Battery backup is very less

From the research analysis, it can be concluded that most IoT communication protocols are of two types. One is Sensor-specific-network protocols (which are used within IoT devices for communication purposes), and the other is Gateway-specific-network protocols (which are used to route the data from the internet or LAN to low power lossy network or vice versa). Table 2 shows the advantages and disadvantages of most communication protocols used more frequently to provide secure communication in IoT deployment.

6. Conclusion

In the last few years, there has been a huge evolution in the IoT field. But still, IoT system is facing lots of threats and challenges from different sides. Here, the in-depth review and analysis of the IOT structure, its security aspect and requirements, and the cause of vulnerabilities are elaborated. in addition, the research status in the security-privacy, encryption mechanism, and communication security of IoT infrastructure is discussed here. Furthermore, an improvised security architecture for IoT paradigms is proposed, which can enhance the security downside of the IoT framework, and a combined secure protocol stack is elaborated.

Future work

The in-depth analysis of security issues and discussion of its corrective measures are done here. A details analysis and practical developments of security measures will be done in the future.

Acknowledgments

All authors and publishers whose research have been referred to and cited in this paper are acknowledged with lots of gratitude. the author of this paper is obligated to the Editor and the reviewer for their recommendations which make us improve the eminence of the paper.

References

[1] International Telecomunicaciones Union (Itu), 2012.Recommendation Itu-T Y.4000/Y.2060, (2012)
[2] X. Jia, O. Feng, T. Fan, and Q. Lei, Rfid Technology and Its Applications in Internet of Things (Iot), in Proc. 2nd Ieee Int. Conf. Consum.Electron., Commun. Netw. (Cecnet), Yichang, China, (2012) 1282–1285.
[3] S. Li, L. Xu, and X. Wang, Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things, Ieee Trans. Ind.Informat., 9(4) (2013) 2177–2186, Nov. 2013.
[4] W. He and L. Xu, Integration of Distributed Enterprise Applications:A Survey, Ieee Trans. Ind. Informat., 10(1) (20140 35–42,Feb. 2014.
[5] K. Ashton Et Al., That Internet of Things Thing, Rfid Journal, 22(7) (2009) 97–114, 2009.
[6] Koshizuka, N.; Sakamura, K. Ubiquitous Id: Standards For Ubiquitous Computing and the Internet of Things. Ieee Pervasive Comput, 9 (2010) 98–101.
[7] Want, R. An Introduction to Rfid Technology. Ieee Pervasive Comput, 5 (2006) 25–33.
[8] Want, R. Near Field Communication. Ieee Pervasive Comput, 10 (2011) 4–7.
[9] Mcdermott-Wells, P. What Is Bluetooth? Ieee Potentials , 23 (2004) 33–35.
[10] I.Mashal,O.Alsaryrah,T.-Y.Chung,C.-Z.Yang,W.-H.Kuo,and D. P. Agrawal, Choices For Interaction with Things on Inter-Net and Underlying Issues, Ad Hoc Networks,28 (2015) 68–90,2015.
[11] G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, Security Characteristic and Technology in the Internet of Things, Journal of Nanjing University of Posts and Telecommunications (Natural Science), 30(4) (2010).
[12] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, Future Internet:the Internet of Things Architecture, Possible Applications Andkey Challenges, in Proceedings of the 10th International Conference on Frontiers of Information Technology (Fit '12), (2012) 257–260, December 2012.
[13] Iotsploit – Iot Vulnerability Scanner — Iot Firmware Analyzer —Iotpentesting and Security Consultiung, Https://Iotsploit.Co/, Accessed: (2022).
[14] R. H. Weber, Internet of Thingsnew Security and Privacy Challenges. Amsterdam, the Netherlands: Elsevier, (2010).
[15] D. Kozlov, J. Veijalainen, and Y. Ali, ``Security and Privacy Threats in Iot Architectures," in Proc. 7th Int. Conf. Body Area Netw., (2012) 256262.
[16] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, Future Internet:the Internet of Things Architecture, Possible Applications Andkey Challenges, in Proceedings of the 10th International Conference on Frontiers of Information Technology (Fit '12), (2012) 257–260, December 2012.
[17] H. Suoa, J. Wana, C. Zoua, and J. Liua, Security in the Internet of Things: A Review, in Proc. Int. Conf. Comput. Sci. Electron. Eng., 2012, Pp. 648651. [14] A. Cooper, Security For the Internet of Things," School Comput.Sci. Commun., Kth Royal Inst. Technol., Stockholm, Sweden, Tech.Rep. 848663, (2015).
[18] Https://Barbaraiot.Com/Blog/Main-Attacks-Malware-Iot-Devices-2018, Accessed: 02-Feb-2022.
[19] K. Angrishi, Turning Internet of Things (Iot) Into Internet of Vulnerabilities (Iov): Iot Botnets, Arxiv Preprint Arxiv:1702.03681, (2017).
[20] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, Internet of Things (Iot) Security: Current Status, Challenges and Prospective Measures,in Proc. 10th Int. Conf. Internet Technol. Secured Trans. (Icitst), London, U.K., (2015) 336–341.
[21] J. Zhao, on Resilience and Connectivity of Secure Wireless Sensor Networks Under Node Capture Attacks, Ieee Trans. Inf. Forensics Security, 13(3) (2017) 557–571.
[22] W. Trappe, R. Howard, and R. S. Moore, Low-Energy Security: Limits and Opportunities in the Internet of Things, Ieee Security Privacy, 13(1) (2015) 14–21.
[23] D. G. Costa, I. Silva, L. A. Guedes, F. Vasques, and P. Portugal, Availability Issues in Wireless Visual Sensor Networks, Sensors, 14(2) (2014) 2795–2821.
[24] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, Dtls Based Security and Two-Way Authentication For the Internet of Things, Ad Hoc Netw., 11(8) (2018) 2710–2723, 2013.
[25] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, Pauthkey: A Pervasive Authentication Protocol and Key Establishment Scheme For Wireless Sensor Networks in Distributed Iot Applications, Int. J. Distrib. Sensor Netw., 10(7) (2014) 357–430, 2014.
[26] B. Wei, G. Liao, W. Li, and Z. Gong, A Practical One-Time File Encryption Protocol For Iot Devices, in Proc. Ieee Int. Conf. Comput. Sci.Eng. (Cse) Embedded Ubiquitous Comput. (Euc), 2 (2017) 114–119.
[27] L. Markowsky and G. Markowsky, Scanning For Vulnerable Devices in the Internet of Things, in Proc. Ieee 8th Int. Conf. Intell. Data Acquisition Adv. Comput. Syst. Technol. Appl. (Idaacs), 1 (2015) 463–467.
[28] C. Konstantinou and M. Maniatakos, Impact of Firmware Modification Attacks on Power Systems Field Devices, in Proc. Ieee Int. Conf. Smart Grid Commun. (Smartgridcomm), Miami, Fl, Usa, (2015) 283–288.

[29] Q. Feng Et Al., Scalable Graph-Based Bug Search For Firmware Images, in Proc. Acm Sigsac Conf. Comput. Commun. Security, (2016) . 480–491.
[30] S. L. Keoh, S. S. Kumar and H. Tschofenig, Securing the Internet of Things: A Standardization Perspective, in Ieee Internet of Things Journal, 1(3) (2014) 265-275, June 2014, Doi: 10.1109/Jiot.2014.2323395.
[31] N. Krishnaraj, S. Sangeetha A Study of Data Privacy in Internet of Things Using Privacy Preserving Techniques with Its Management International Journal of Engineering Trends and Technology 70.2(2022):43-52. Doi:10.14445/22315381/Ijett-V70i2p207
[32] Pongle, P., & Chavan, G. (2015). Real Time Intrusion and Wormhole Attack Detection in Internet of Things. International Journal of Computer Applications, 121(9) (2015) 1–9. Doi:10.5120/21565-4589.
[33] Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Taeshik Shon, Hafiz Farooq Ahmad,A Lightweight Message Authentication Scheme For Smart Grid Communications in Power Sector, Computers & Electrical Engineering, Volume 52,2016,Pages 114-124,Issn 6,Https://Doi.Org/10.1016/J.Compeleceng.2016.02.017
[34] Ma, H., & Chen, B. (2016). An Authentication Protocol Based on Quantum Key Distribution Using Decoy-State Method For Heterogeneous Iot. Wireless Personal Communications, 91(3) (2016)1335–1344. Doi:10.1007/S11277-016-3531-2.
[35] Tewari, A., & Gupta, B. B. (2016). Cryptanalysis of A Novel Ultra-Lightweight Mutual Authentication Protocol For Iot Devices Using Rfid Tags. the Journal of Supercomputing, 73(3) (2016) 1085–1102. Doi:10.1007/S11227-016-1849-X.
[36] R. Stephen and L. Arockiam , Intrusion Detection System to Detect Sinkhole Attack on Rpl Protocol in Internet of Things," Int. J. Elect. Electron.Comput. Sci. Eng., 4(4) (2017).
[37] T. H. Lin, C. C. Lee, and C. H. Chang, Wsn Integrated Authentication Schemes Based on Internet of Things," J. Internet Technol., 19(4) (2018) 1043-1053.
[38] F. Y. Yavuz, D. Ünal, and E. Gül, Deep Learning For Detection of Routing Attacks in the Internet of Things," Int. J. Comput. Intell. Syst., 12 (1) (2018) 39 58, Nov. 2018. Doi: 10.2991/Ijcis.2018.25905181.
[39] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, ``Continuous Patient Monitoring with A Patient Centric Agent: A Block Architecture," Ieee Access, 6 (2018) 32700-32726, 2018. Doi: 10.1109/Access.2018.2846779.
[40] G. Liu,W. Quan, N. Cheng, H. Zhang, and S.Yu, Efficient Ddos Attacks Mitigation For Stateful Forwarding in Internet of Things, J. Netw. Comput. Appl., 130 (2019)113. Elsevier Doi: 10.1016/J.Jnca.2019.01.006.
[41] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, Token-Based Lightweight Authentication to Secure Iot Networks, in Proc. 16th Ieee Annu. Consum. Commun. Netw. Conf. (Ccnc), (2019) 1-4. Doi: 10.1109/Ccnc.2019.8651825.
[42] Mostafa, A., Lee, S. J., & Peker, Y. K. (2020). Physical Unclonable Function and Hashing Are All You Need to Mutually Authenticate Iot Devices. Sensors, 20(16) (2020) 4361. Doi:10.3390/S20164361.
[43] Smita Sanjay Ambarkar, Narendra Shekokar An Efficient Authentication Technique to Protect Iot Networks From Impact of Rpl Attacks International Journal of Engineering Trends and Technology, 69(10) (2021) 137-145. Doi:10.14445/22315381/Ijett-V69i10p217
[44] H. Ning and Z. Wang, Future Internet of Things Architecture: Like Mankind Neural Systemor Social Organization Framework? Ieee Communications Letters, 15(4) (2011) 461–463.
[45] M. Aazam and E.-N. Huh, Fog Computing and Smart Gateway Based Communication For Cloud of Things, in Proceedings of the 2nd Ieee International Conference on Future Internet Ofthings and Cloud (Ficloud ’14), (2014) 464–470. Barcelona, Spain, August 2014.
[46] Burhan, Muhammad, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim. Iot Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors , 18(9) (2018) 2796.
[47] Peña, M. A. L., & Fernández, I. M. (2019, April). Sat-Iot: An Architectural Model For A High-Performance Fog/Edge/Cloud Iot Platform. in 2019 Ieee 5th World Forum on Internet of Things (Wf-Iot), (2019) 633-638. Ieee.
[48] J. Soldatos, N. Kefalakis, M. Hauswirth Et Al., Openiot: Open Source Internet of-Things in the Cloud, in Interoperability and Open-Source Solutions For the Internet of Things: International Workshop, Fp7 Openiot Project, Held in Conjunction with Soft- Com2014, Split, Croatia, September 18, 2014, Invited Papers, Vol. 9001 of Lecture Notes in Computer Science, (2015) 13–25.Springer, Berlin, Germany.
[49] A. Ranganathan, J. Al-Muhtadi, S. Chetan, R. Campbell, and M. D. Mickunas, Middlewhere: A Middleware For Location Awareness in Ubiquitous Computing Applications, Inacm/Ifip/ Usenix International Conference on Distributed Systems Platforms and Open Distributed Processing Middleware , (2004) 397–416. Springer, New York, Ny, Usa.
[50] M. Eisenhauer, P. Rosengren, and P. Antolin, A Development Platform For Integrating Wireless Devices and Sensors Into Ambient Intelligence Systems, in Proceedings of the 6th Ieee Annual Communications Societyconference on Sensor,Mesh Andadhoc Communications and Networks Workshops (Secon Workshops ’09), (2009) 1–3. Ieee, Rome, Italy.
[51] T. Zahariadis, A. Papadakis, F. Alvarez Et Al., Fiware Lab: Managing Resources and Services in A Cloud Federation Supportingfuture Internet Applications, in Proceedings of the 7th Ieee/ Acm International Conference on Utility and Cloud Computing (Ucc ’14), (2014) 792–799. Ieee, London, Uk, (2014).