Security Issues In Different Layers Of IoT And Their Possible Mitigation

[1]Debabrata Singh, [2]Pushparaj, [3]Manish Kumar Mishra, [4]Anil Lamba, [5]Sharabanee Swagatika

Abstract— Internet of things (IoT) is a new paradigm merging with the social networks, allowing information sharing between smart people and smart devices. It is also intended for ubiquitous connectivity among various entities or things through Internet. However security and privacy issues are great challenges for IoT. The heterogeneous technologies, intrinsic vulnerabilities of IoT devices, lack of designed IoT standards welcomes the cyber attacks. The main goals of this analytical study are to bring the various security challenges & issues on different layers of IoT architecture and their possible solutions. Also provide a taxonomic presentation of the main three layers IoT system model with their protocol stack. As a result, we highlight the most challenging security issues and their mitigation with some future research directions.

Index Terms— Data privacy, attack, Cloud computing security, content protection, data hiding, data privacy, firewall security.

1 INTRODUCTION

INTERNET of Things (IoT) is one of the key components of digital and transformation of digital world along with Social, Mobile, Analytics and Cloud (SMAC). It is otherwise called as Internet of Everything or Industrial IoT. IoT, Big Data and SMAC can helps as a numerous possibilities that were unheard earlier. It takes the absolute center stage for the product vendors, system integrators, software companies and IT sector companies. Today's Industry analysts says, there will be around 26 billion devices on the IoT(Cisco estimate 50 billion) by the end of 2020 and the data exchange will be 40 Zettabytes over the networks[1]. According to the McKinsey Global Institute, IoT market will have a potential impact of $3.9tn- $11.1tn per year by 2025 over various applications i.e. smart cities, smart industries, home, offices, retail environments, worksites, human health, logistic& navigation, and smart vehicles[2] . The abstract level of IoT model contains various physical devices, or sensors i.e. controllable sensors, RFID (Radio Frequency Identifications), IoT getaways, web servers [3] as depicted in Figure 1.

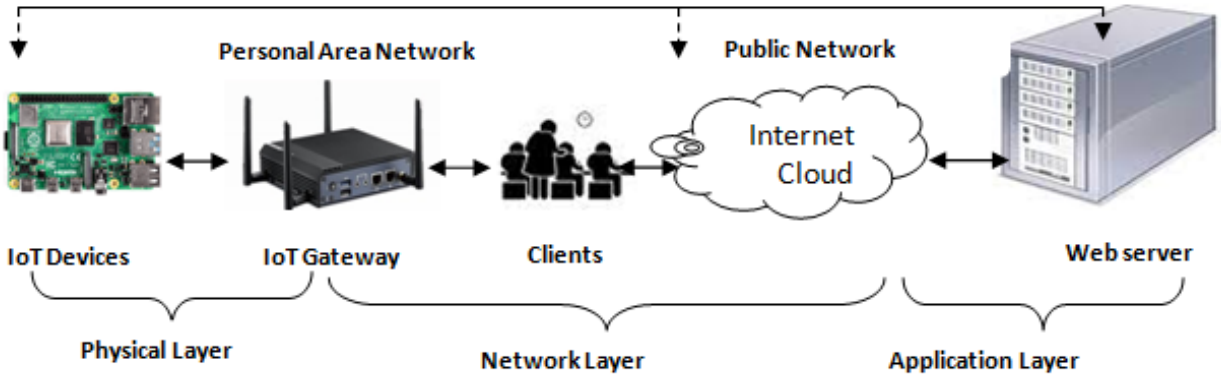


Figure 1. Abstract level of three layer architecture of IoT

The term "things" from IoT comprises both the physical world (physical events, objects, behaviors, and tendencies) and cyber world (cyber events, actions, entities, and solutions) [4]. IoT brings up many challenges and holds much promise i.e. the data generated, stored or transmitted through IoT devices, so many security issues & privacy of the users can have serious consequences. Every challenge to the IoT system must be secured, controllable and privacy to the smart users, only when the IoT systems are built up with security. The general architecture of an IoT system is divided with three layers i.e. i) Physical layer/Perception Layer, ii) Network Layer & iii) Application Layer. The three layer architecture of IoT system is depicted in Figure 1. The deployment process involves various technologies i.e. WSNs, RFID, Bluetooth, NFC [5], IP, EPC (electronic product code), Wi-Fi & various actuators [6].The intelligent and smart applications of IoT interconnected devices helps personal as well as economic benefits to the society[7]. In this paper we discussed the different levels of IoT system as well as the protocol stack of IoT system, security challenges & vulnerabilities of various underlying techniques. Section 2 represents the security issues on IoT with their challenges, & study some security related works under Section 3. IoT Reference model described under Section 4 and IoT protocol stack presentation is in Section 5. Different types of attacks in IoT system model are presented in Section 6 and different layer attacks with their possible solutions are presented in Section 7. Finally we summarize the content to give a clear picture of ongoing security issues, challenges and their possible solutions.

2. Security Issues on IoT

In IoT many sensor devices and smart peoples are connected with each other through Internet to provide services at anytime, anywhere, and any types of services. IoT also provide services at any business, anybody, any one, any context, any device, anything, any path and any Network. Owing to the wide range of impact on daily life, all the sensor devices are connected through Internet and all are also

vulnerable to all privacy and security issues like authenticity, confidentiality and integrity tec. Security in the field of Information Technology (IT) [8-10] considers three features: confidentiality, integrity, and availability as the prime objectives and are called as CIA triad [11]. Security is defined as a process by which unauthorized access to the system state is prevented and thus the privacy is not compromised. Confidentiality refers to the secrecy of data, whereas integrity confirms that the data is not changed in transmission [12][13]. Further, availability provides the smooth transmission of data whenever it is required. In a secure network some of the required capabilities are:

i. Data Authentication: The sensed data & related information collected from secured, authenticated devices must be followed some technical mechanism & allow to transmit.
ii. Resilience to attacks: During data transmission if the system crashes, it should be automatically recover itself as same data uses in different domain. A cloud server must be protect smartly & intelligently himself from an intruders or eavesdropper.
iii. Client Privacy: At client side, the used data & information must be secure and safe. Personal data should be accessed by privately through the authorized person and maintain the privacy. The private data should be protected i.e. no irrelevant authenticated user or other types of client can't be access the private data from the client.
iv. Access control: Only authenticated and authorized person can access the control. The general user can access the system by providing user name and password & their access rights, which will be controlled by the system administrator. Different user can access the specific portion of the database or programs to smoothen running the system.

Security issues are divided into different sub-categories, viz., data confidentiality, monitoring and tracing of activities, avoidance of malicious insiders, hijacking of services or processes including phishing, lack of transparency into providers' service provisions and procedure environments, fraudulent activities and exploitation, management of multi-instance in multi-tenancy etc. [14][15]. Moreover, probability of attack through side channel, escaping the sandboxed environment, can access the virtual machine and hence unauthorized or spoofed access to the host are also a possibility [16-18]. Encryption techniques are also the most important tool in providing multidimensional security services for IoT [19].

2.1 IoT Security Issue Challenges

In IoT mostly, application data are person concern, industrial and enterprise. These application data must be secured and confidential against any kind of theft and tampering [20]. The biggest challenging factor in IoT is security. Security is a concern where data is securely transmitted over the communication channel in the network. The IoT improve the communication between devices but still there are so many issues for time (response time), scalability, and availability. IoT incorporate transparently and seamlessly a large number of different and heterogeneous end system, while providing open access to selected subsets of data for the development of a plethora of digital services. It happens due to extremely large variety of devices and link layer technology. In IoT though machine to machine technology is the first phase, but it enables new applications and to bridge diverse technology by connecting physical objects together in support of intelligent decisions. Open Web Application Security Project (OWASP) has defined ten top security issues associated with IoT devices i.e i) Insecure network services, ii) Insecure web interface, iii) Insufficient authentication or authorization, iv) Lack of transport encryption, v) Privacy concern, vi) Insecure cloud interface, vii) Insecure mobile interface, viii) Insufficient security configuration, ix) Insecure software or firmware and x) Poor physical security[21].

Among different security challenges, the important and most challenges are:

1. Data Privacy & Security: While transmitting data seamlessly, data must be secure from theft and hide from the hackers.
2. Insurance Concerns: The insurance companies installing IoT devices on any application oriented a device which collects data to take decisions about insurance.
3. Technical Concern: Due to excess use of IoT devices, the traffic generated by these devices is also increasing. So it must need a larger network capacity, which requires storing the huge amount of data for analysis and store.
4. Lack of common Standard: Since there are many standards for IoT devices and many IoT companies, authorized and unauthorized devices connected to the IoT system are most challenging factor.
5. Security attacks and System Vulnerability: IoT system mainly focus on different security challenges, to design proper guideline for security of a network and different security frameworks i.e. system security. To handle IoT applications we require application security and network security helps in securing IoT communication network for communication of different IoT devices.

3. Related Work

Mario Frustaci et al. [21] describe the order on IoT security in the different layers of IoT. The authors taxonomically analyze the three key layers of IoT system model i.e perception (Physical layer), transportation (Network layer) and application levels (Application layer). Their approach represents a fertile ground to overcome the cyber threats. The main goal is how security will be provided to support the IoT paradigm. Due to limited resources and technological heterogeneity these strategies' and generic policy must be redesigned to address the IoT. Shivang vashi et. al. [22] also finds the security problem in IoT layers (three main layers i.e perception, transport and application). The main problem in perception layer includes leakage of information's, terminal virus, tampering and copying etc. The network content security hackers process, illegal authorizations are the main challenges in transport layer. This transport layer also describe some security i.e. cyber, sinkhole, sleep deprivation, dos and man in the middle. But application layer guarantee the integral, controllability and authenticity of the data. This layer also focus on malicious code injections, DoS, Spear phishing, Sniffing etc.

Kiwoony Kwon et al. [23] deals with some security issues as well as performances of IoT. In this paper the author proposed an Oliot-Discovery Service(DS) for the purpose of security this intra-approach describe fine -grained access contra model followed by two layer stage model. The Intra-DS mainly provides three services i.e access control, main storage and cache services. The access control service cheek's the user authentication data of things in main storage services. But in cache service maintain both access control & main storage services, which also query about the exiting data and back-end database for cache misses. Oliot-Discovery Service prevents unauthorized access and provides durability against many operations. V. Kherechenko et al. [24] focused on the security issues in smart business center(SBC).In this paper the author mainly focus on reliability & security at different levels .ie. Communication several level and SBC sub system. The author also relates this technical condition of SBC network's component with the Marker's Model. Finally they analyzed the statistics of failures of S/W & H/W with protective against hacker attacks as well as high security. The authors also developed a model which provides the reliability to the user and safety to the SBC hardware. Kozlov et al. in [25] describe in their survey, about the new threats for the security issues at different levels of IoT architecture. The author analyzes the high level threat selection by considering application domains and many scenarios i.e. mobile apps, smart energy, smart home, and road transportation. Mainly the authors focus on the energy issues as well as the threats at the lowest level of IoT. Lastly they elaborate the private & security area through EU legislation (one individual can control all the levels of the architecture, if he/she get the data & information).

4. IoT Reference Model

The reference model of IoT can be represented by seven levels. The levels are:

1. Physical devices & controllers(The ' things' in intelligent engineering)
2. Connectivity (communication & processing unit)
3. Edge computing(Data element analysis & transformation)
4. Data accumulation(Storage)
5. Data abstraction(Aggregation & access)
6. Application(Reporting& analysis control)
7. Collaboration & processes(Involving people & business processes)

Broadly different levels of an IoT system can be described as:
Level-1: IoT system has a single device that performs sensing and/or actuation, performs analysis stores data and host the applications. These levels are suitable for modeling low complexity and low cost solutions where the data is medium and analysis requirements are computationally extensive. Mostly these are used in home automation. A level-2: IoT system has same as level-1 IoT system but it included local analysis. Data stored at the cloud and application is usually cloud-based. These systems are more suitable for solution where the data involved is big and the requirement is same as level-1 IoT. Mostly these are used in smart irrigation. But in Level-3 IoT system has same as level-1 and 2 but data can be stored and analyzed in cloud and cloud-based applications. These system levels are involved in big data analysis and computationally intensive requirements as depicted in Figure 2. level-4 IoT system has multiple nodes that perform local analysis, i.e. cloud-based application where data's are stored in the cloud and observer nodes (not performing any control functions). The observer node can subscribe to and receive information collected in the cloud from the IoT devices and also process information. These are more applicable for big data, and used in requirements are computationally intensive with requirement of multiple nodes. Mostly we used these levels for noise monitoring. Level-5 IoT system has multiple nodes with one coordinator node which collects data from the end nodes and sends to the cloud. The end node helps in sensing and/or actuation. These are mainly implemented in forest fire detection. Data are stored, analyzed in the cloud database and applications are cloud-based as in level-4. These level-5 systems data are big and requirement analyses are computationally intensive.

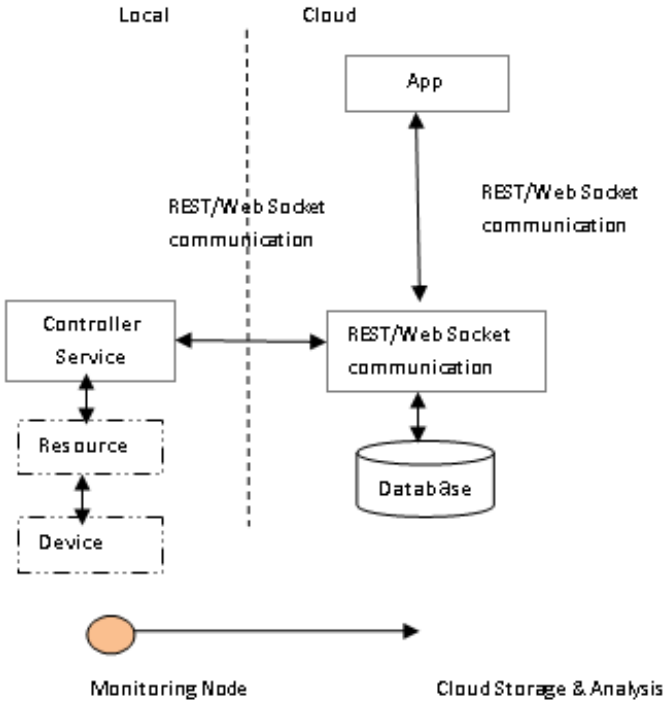


Figure 2. IoT level 1, 2, 3

But in level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and data sends to the cloud. Data are stored in the cloud (cloud database) and supports cloud-based applications as depicted in Figure 3. In Level-7, the results are visualized with the cloud-based application. The centralized controller is aware to all end nodes and sends control commands to the nodes. Mostly these are used in weather monitoring. The end node contains various sensors i.e. temperature, pressure and humidity. These end nodes send the data to the cloud in real-time using a Web Socket service. The data analyses are done in the cloud by using cloud database. To make a prediction we aggregate the data in a cloud-based application which are visualized in the cloud-database.

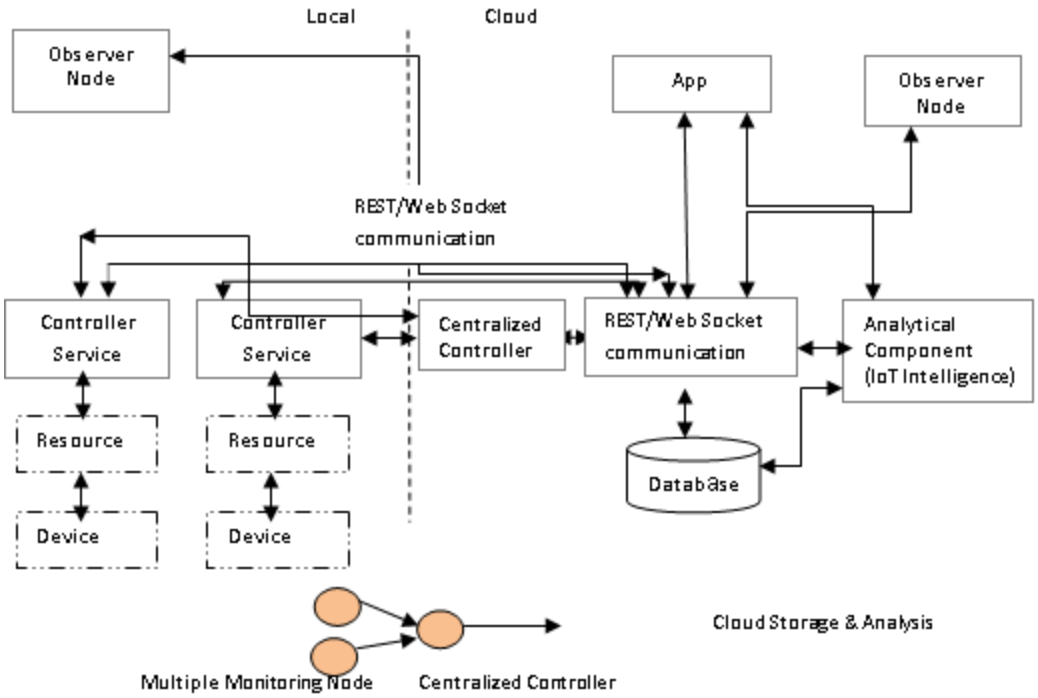


Figure 3. IoT level 4, 5, 6 & 7

5. A Protocol Stack for the IoT

Currently, in Internet network all the security and communication related problems are solved using IoT based application developed by some standardized bodies like Internet Engineering Task Force (IETF)[26] and Institute of Electrical and Electronics Engineers (IEEE)[27,28]. The standardized IoT protocol stacks are depicted in Figure 4. Different layers of protocol stacks with their protocols are:

5.1 Physical/Link Layer: Like IEEE 802.11(WAN), IEEE 802.15.4 is a standard wireless communication, which defines the physical (PHY) as well as Logical layer (MAC) Medium access control layer. 802.15 groups specify a group of wireless personal area (WPANs) networks for different applications [29]. It focuses on communication between low resources like power, memory & bandwidth, with constrained environment devices.

5.4 IoT Convergence Protocols in Application Layer: In IoT, to convey the contained information the convergence protocol supports information exchange in one domain to another domain [35]. Generally there are two types of data exchange protocol architectures are available in IoT i.e. broker based (message centric) and bus based (data centric). In broker based architecture, the broker controls the information distribution i.e. information store, filters and forwards, prioritizes publish, transmission of message from client to subscriber and vice versa. These protocols are also called message centric protocols which helps in deliver the message to the recipients. Some of the broker based protocol (Data exchange protocol) includes:

a) AMQP- Advance Message Queuing Protocol emerged in financial field for replacing exclusive and non-comparable message systems. It helps in queuing, routing, message orientation, security and reliability. It also provides message-delivery guarantees, authentication, encryption and flow controlled.

b) CoAP- Constrained Applications Protocol: It is a client/server internet-based protocol designed for constrained devices which is similar like HTTP. It is designed for interoperability with the web and asynchronous communications. It works in the concept of peer to peer which uses UDP as its transport layer protocol making the transmission faster.

c) MQTT- Message Queue Telemetry Transport used TCP as its transport layer protocol due to its longtivity. It helps in asynchronous communications and used for two way communications over unreliable returns. Due to the data negotiation, partial interoperability between publisher and subscribers are guaranteed. For this it compress the message using an application efficient XML interchange (EXI).

5.2 Network layer: In IEEE 802.15.4 allows larger IPv6 packets through 6LoWPAN (Low power wireless personal area network). Without 6LoWPAN IPv6, an Internet protocol doesn't work on LoWPAN. It controlled by Internet engineering task forces (IETE) and defines many open standard protocols i.e. UDP, TCP & HTTP. IPv6 helps in packet encapsulation, packet fragmentation, header compression & reassembly the fragmented packets to recreate the original IPv6 packets. Finally link layer forwards the packets to transport layer.

5.3 Transport Layer: In transport layer TCP is used for Internet and UDP is used for gaming and video streaming. Most IoT scenarios are well suited for UDP, which is lighter than TCP. UDP is much faster, connection protocol and guaranteed packet delivery. Header size of UDP is much smaller than TCP. In IoT protocols i.e. CoAP higher level application layer uses UDP instead TCP.

d) JMS- Java Message Service API: It is an application oriented Java Enterprise Edition for create, send, receive, read and write to many clients at a time. It helps to eliminate between distributed applications and helps to separate transport layer to application layer. It also used to communicate in JMS provider.

But in bus-based architecture, there is no centralized broker concept. Here clients publish their messages to the subscribers on a specific topic. These are called data centric protocols which focus on data delivered at the receiver end. Some of the bus-based protocols are: i) DDS- Data Distribution Service, ii) REST- Representational State Transfer and iii) XMPP- Extensible Messaging & Presence Protocol.

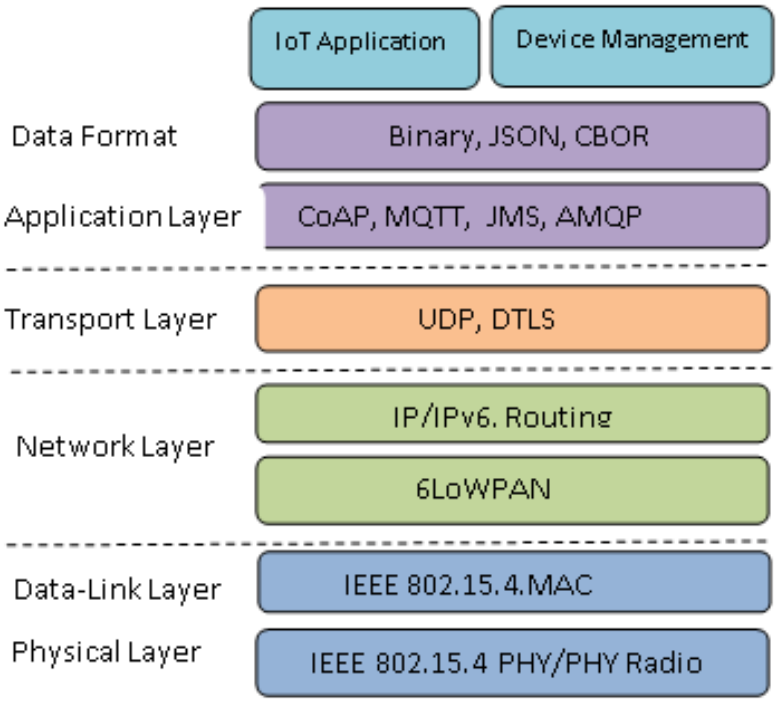


Figure 4. The standardized IoT protocol

6. Attacks and Threats in IoT system model

In IoT system model different layers of IoT are facing various attacks including active and passive attacks. The attacks can be of two types depending on their behavior in network i.e. active and passive attacks [31]. Network behaviors are

i. **Active attack:** The attacker disturbs the performance of the network by stealing the data at the time of communication in active attack.

ii. **Passive Attack:** The communications channels are observed and form its usage history the passive attacker steal the information [31].

As discussed earlier, IoT framework model can be spoken to by three principle layers for example Physical, system and application layer. Every one of these layers abridged in Figure 5, has its own innovations and some security shortcomings. The security problems of each layers are discussed with possible threats and next part of this section, we discussed the feasible solutions to that threats.

6.1 Attacks in Physical/Perception Layer

The physical layer incorporates sensors and actuators to perform estimation of temp, speeding up, mugginess and functionalities like questioning area [32]. The fundamental security dangers in physical layer are because of constrained hub assets and appropriated composed structure. The main threats are:

i. Tampering: These attacks generally focused on hardware components and the attacker needs to be physically present into the IoT system & continue its process to make system busy. A few models are hub altering and vindictive code infusion. In hub altering assailant can harm the sensor hub by electronically denies to get to, alter the sensitive information or physically replace the part of its hardware or entire node. But in malicious code injection, the attacker injects its malicious code physically on to a node and access to that node from that IoT system.

ii. Impression: Authorization/ Validation in the disseminated systems are so troublesome. So enabling malevolent hub to make a phony distinguishing proof for noxious assaults.

iii. Denial of Service (DoS): Attackers adopt the finite processing ability of the nodes, to make the system unavailable.

iv. Routing attackers (WSN, RSN): In the Data collection and forwarding process, intermediate malicious node modify the routing path and make the system busy.

v. Data transit attacks (in WSN/RSN): Various attacks like sniffing, Man in the middle attacks on the integrity & confidentiality during data transit.

6.2 Attacks in Network & Transport Layer

System layer gives universal access condition to the physical layer. It get the information from physical layer and transmit

the assembled data to a specific data framework through Internet or access systems [33].The important security threats are:

i. Routing attacks: during the data collection & forwarding process intermediate malicious nodes may modify the routing path and get system infected.
ii. DoS attacks: In network layer vulnerable attacks are due to heterogeneity and complexity of IoT networks. Exhaustion, collision and unfairness are the three important methods in DoS attacks.
iii. Data transit attacks: In core networks, during data transit, various attacks occur on the data integrity and confidentiality.
iv. Spoofed Routing information: Attackers spoof, alter or replay IP address to disturb the traffic in the networks, resulting routing loops, fake error message, and shortened routes etc.
v. Selective forwarding: A malignant or altered hub may change the IP of the traffic by dropping some message and sending others, subsequently debased. Man in the Middle attacks: When the attackers jamming to access the information for his advantage. It mainly contains three types of attacks like:
vi.
    a) Eavesdropping: It's a passive attack, where attacker can access the communication channel & alter the received packets and send to all.
    b) Directing assault: assailants may change the steering data and make steering circle to essentially decay the nature of administrations.
    c) Replay attacks: Attackers capture a signed packet & gain the trust of the destined entity by resending later to the sender. It changes the message sequence numbers &authentication code and also acts as real sender.

6.3 Attacks in Application Layer

Application layer provides the services as per request by the customers. The significance of this layer for the IoT is the capacity to give superb brilliant administrations to IoT applications. Different IoT environments can be implemented in their application layer. The Application Support Sub layer (ASS) underpins a wide range of business administrations, asset assignment, canny calculation and can be implemented through specific middleware as well as cloud computing platforms [34]. In this layer the main attacks are:

i. Data leakage: The interloper/assailants can without much of a stretch take the secret phrase or mystery information by knowing the vulnerabilities of the service or applications.
ii. DoS attacks: The interloper/attackers can demolish the accessibility of administrations or application itself.

Malicious code injection: The intruder/ attackers can upload their malicious code into the software applications, to get system infected and exploiting the layer vulnerable to get attacked.

7. IoT Layer attacks and their possible solutions

Sometimes active attacks/vulnerable attacks can prevent the IoT devices smartly. Prevention of IoT devices from the vulnerable attacks can be done by deploying some security constraints [39,40]. According to the behavior, different categorized attacks are:

a) Low level attack -When network is attacked by intruders and that & it's attack is not secure)
b) Medium Level attack-When intruders are listening to the medium while changing the data integrity.
c) High level attack-When intruders is carried on a network & it alters the intensity as well as modify the original data)
d) Extremely High level attack -When Intruders attack on the network with the adoption of unauthorized access and doing the illicit operations leading to suspended or unavailability of networks or congestion of the network.

In 7.1 we present IoT layer protocols: issues and their solution and security threats in automation of IoT and probable mitigations are discussed in section 7.2

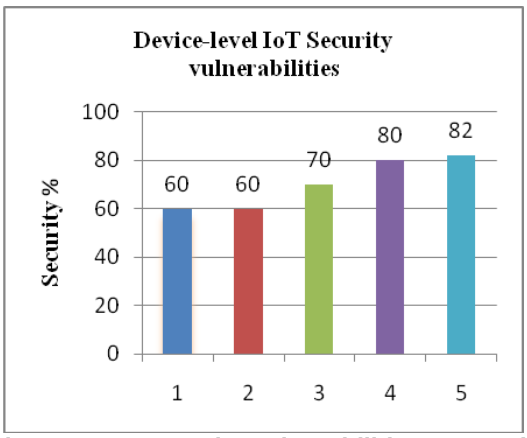
7.1. IoT Layer Protocols: Issues and Their Solution

Layer/Level	Protocols	Issues	Solutions
Physical Layer	IEEE 802.15.4	Data Transit Attacks	AES-CCM algorithms [39]
	BLE	Data Transit Attacks: header type	Black network solution [36]
	Wi-Fi, LTE	Data Transit Attacks	WEP, WPA2 protocols [36] EEA and EIA algorithms [37]
Network Layer	IPv4/IPv6	Threats to NDP protocol	SEND protocol in IPv6 [38]
	6LoWPAN	Data Transit Attacks	Compressed DTLS [39]
	RPL	Routing and DOS Attacks	SVELTE IDS solution [40]
Application Layer	MQTT	Data Transit Attacks, Scalable Key management	Secure MQTT solution with ABE[42],Sec Kit Solution [41]
	CoAP	Data Transit Attacks,	Lithe solution[42]
	AMQP	Switching, Reliability, message orientation, & queuing	subscriber Or publisher models[43]
	XMPP	gaming, multi-party chatting & voice/video calling	client-server and server-server communication paths[43][45]
	DDS	Publish/subscribe model	real-time communication [44]

7.2. Security Threats in IoT Automation and Their Possible Mitigation

Layer	Threat Type	Mitigation
Physical	Tampering	Tamper-resistant packaging
	Denial of Service	Spread-spectrum techniques
	Physical Attacks	Shared cryptographic & Keys or routing tables
	Impersonation	AES-CCM algorithms
	Routing Attacks & Data Transit Attacks (e.g. in WSN, RSN)	WEP, WPA2 protocols, Black network solution
	Firmware Alteration	Use physical access control for update procedure
	Jamming	Channel surfing, priority messages, & spatial retreat
	Radio interference	Delayed disclosure of keys
	Tampering	Tamper proofing, hiding
	Collisions	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
	OS/Software Vulnerability	Educate R&D people on security and conduct product test.
Networking (Data Processing)	Denial of Service	Traffic control, Link Authentication, Active firewalls, & passive monitoring (probing)
	Eavesdropping	Encryption, authorization
	Data Transit Attacks	Compressed DTLS
	Back door attack	At entry point in all system must be properly configured firewalls
	Social Engineering	Awareness about security& its mechanism to the employee
	Exhaustion	Traffic monitoring
	Malware	Malware detection
	De-synchronization	Authentication
	Flooding	Client puzzles
	Sink-hole	Geo-routing protocol
	Worm-hole, black hole	Authorizations, monitoring redundancy
	Homing	Encryption
	Misdirection	Authorization , Egress filtering, & monitoring
	Phishing or Pharming	Using SSL to assure genuineness of displayed sites.
	Data Wiretapping	Protect communication via IPSEC, SSL/TLS.
Application Level	Client app.	Anti-virus filtering
	Data Leakage	Lithe solution
	DoS Attacks	Secure MQTT solution with ABE
	Malicious Code Injection	Used virus protected S/W and handled the new vulnerabilities
	Comm. channel	Authorization, Proper authentication & Integrity verification
	Integrity, Multi-user access	Testing , planning and process design
	Modifications	Validation
	Data access	Traceability
	User Impersonation Device Impersonation	Using memory card, as a certificate mechanism.
	Overwhelm	Rate-limiting
	Reprogram	Authentication
	Service Interruption	Control access mechanism through network
	Data Alteration	Introducing certificate & access control mechanism.

7.3. Solving the security challenges in Device level



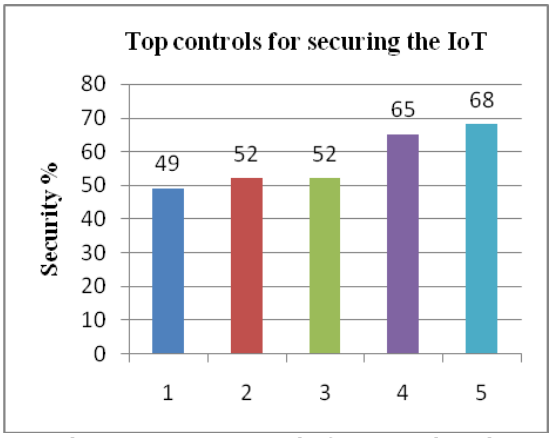


Figure 5. IoT security vulnerabilities on IoT-devices & Figure 6. Top controls for securing the IoT

In designing phase of products the security aspect should be incorporated. The security aspect can be introduced in operating system level and it should be extended through the device stack to the implemented applications and having hardware security capabilities. Generally IoT devices are having 70% security threat and 25% security aspect concerns per device as depicted in Figure 5. As many IoT devices are not designed with security concern in mind it leads to susceptibility and configuration management problem. Figure 6 depicts about the organization's controls for controlling IoT devices.

8. Conclusion

Now a day's IoT seems to be unbeatable and the overwhelming use of smart devices cannot be reversible. Unless and until the security issues are addressed, organizations need to be vigilant, putting appropriate controls, ensuring security risks against the applications and focus on IoT devices those are performing well and who are connected to their networks. The main idea behind this paper is to highlight the security issues & their challenges to the different layers of IoT and deliberating the security concern in various protocols and their possible corrective measures. IoT devices became soft targets as they are deprived of security mechanisms. Security mechanisms should be incorporated to all IoT related devices along with the communication networks. To protect from introducers or threats, we should have used default password & for first time user, install all the security enabled requirements for all the smart devices.

References

[1] Van Der Meulen, Rob, "Gartner says 6.4 billion connected 'things' will be in use in 2016, up 30 percent from 2015", Stamford, Conn (2015).

[2] Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon, "Unlocking the Potential of the Internet of Things", McKinsey Global Institute (2015).

[3] Lamba, A., Singh, S., Singh, B., Sai, S., Muni, R., & Islands, C. (2018). Quantum Computing Technology (QCT) - A Data Security Threat. 5(4), 801–806.

[4] Ning, H. Unit and Ubiquitous Internet of Things; CRC Press, Inc.: Boca Raton, FL, USA, 2013.

[5] Sarangi M, Singh D., Khuntia M., "A potential solution for man-in-middle security issues through near field communication (NFC)", International Journal of Engineering and Advanced Technology (IJEAT), Volume-8(4), pp.492-498, 2019.

[6] Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.

[7] Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012; pp. 257–260.

[8] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, Journal of Internet Services and Applications , vol.4, No.5, 2013.

[9] Arti Ochani, Nilima Dongre, Security issues in cloud computing, International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017

[10] Huaglory Tianfield, Security Issues In Cloud Computing, IEEE International Conference on Systems, Man, and Cybernetics, 2012.

[11] Sammy, F & Vigila, s. (2016), " A survey on CIA triad for cloud storage services", 9, 6701-6709.

[12] Vijaya Lakshmi Paruchuri, "Data Confidentiality in Cloud using Encryption Algorithms", International Journal of Cloud-Computing and Super-Computing, Vol. 3, No. 2, Dec. 2016, pp:7-18.

[13] Lamba, A. (2019). International Journal of Research in Informative Science Application & Techniques (IJRISAT) SR-MLC : Machine Learning Classifiers in Cyber Security-An Optimal Approach International Journal of Research in Informative Science Application & Techniques (I. (3).

[14] A. Chandrika Sai Priya.Integrated Framework for Multi-User Encrypted Query Operations on Cloud Database Services, International Journal of Cloud-Computing and Super-Computing, Vol. 3, No. 2. Dec. 2016, pp:1-6.

[15] Asish Aich and Alo Sen, Study on Cloud Security Risk and Remedy, International Journal of Grid and Distributed Computing, vol.8, no.2, 2015.
[16] Debnath Bhattacharyya, Space and Security Issues in Cloud Computing: A Review, International Journal of Security and Its Applications, vol.12, no.6, 2018, pp. 37-46.
[17] N. Thirupathi Rao, A. Sravani, Debnath Bhattacharyya and Tai-hoon Kim, Security and Assurance Aspects to be Observed in Cloud Computing Based Data Centers: A Study, International Journal of Security and Its Applications, vol.12, no.4, 2018, pp. 1-14.
[18] N. Thirupathi Rao and Debnath Bhattacharyya, Security Aspects to be Considered in Cloud Computing Based Data Centers: A Tutorial, International Journal of Database Theory and Application, vol.12, no.1, 2019, pp. 27-42.
[19] Lamba, A., Singh, S., Singh, B., Sai, S., Muni, R., & Islands, C. (2018). *Quantum Computing Technology (QCT) - A Data Security Threat*. *5*(4), 801–806.
[20] S. Sicaria, A. Rizzardia, L. A. Griecob, and A. Coen-porisinia, “Security, privacy and trust in internet of things: The road ahead,” Computer Networks, pp. 146–164, 2015.
[21] Frustaci, Mario, P. A. C. E. Pasquale, A. L. O. I. Gianluca, and Giancarlo FORTINO., “Evaluating critical security issues of the IoT world: Present and Future challenges”, *IEEE Internet of Things Journal* (2017).
[22] Vashi, Shivangi, Jyotsnamayee Ram, Janit Modi, Saurav Verma, and Chetana Prakash, “Internet of Things (IoT): A vision, architectural elements, and security issues”, In *I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on*, pp. 492-496, IEEE, 2017.
[23] Kwon, Kiwoong, Dongsoo Kim, and Daeyoung Kim, “Oliot-Discovery Service: Dealing with Performance and Security Issues from Intra-DS Aspect for IoT”, In *Global Communications Conference (GLOBECOM), 2016 IEEE*, pp. 1-6, 2016.
[24] Kharchenko, Vyacheslav, Maryna Kolisnyk, Iryna Piskachova, and Nikolaos Bardis, “Reliability and Security Issues for IoT-based Smart Business Center: Architecture and Markov Model”, In *Mathematics and Computers in Sciences and in Industry (MCSI), 2016 Third International Conference on*, pp. 313-318, IEEE, 2016.
[25] D. Kozlov, J. Veijalainen, and Y. Ali, “Security and Privacy Threats in IoT Architectures,” *in Proceedings of the 7th International Conferenceon Body Area Networks,* ICST, Brussels, Belgium, pp. 256–262, 2012.
[26] Rahman, Md Mustafizur, Choong Seon Hong, Sungwon Lee, Jaejo Lee, Md Abdur Razzaque, and Jin Hyuk Kim. "Medium access control for power line communications: an overview of the IEEE 1901 and ITU-T G. hn standards." *IEEE Communications Magazine* 49, no. 6 (2011): 183-191.
[27] Bonaventure, O. "Internet Engineering Task Force (IETF) L. Iannone Request for Comments: 6834 Telecom ParisTech Category: Experimental D. Saucez." (2013).
[28] Yan, Ye, Yi Qian, Hamid Sharif, and David Tipper, “A survey on cyber security for smart grid communications”, *IEEE Communications Surveys & Tutorials* 14, no. 4 (2012): 998-1010.
[29] Aijaz, Adnan, and A. Hamid Aghvami. "Cognitive machine-to-machine communications for Internet-of-Things: A protocol stacks perspective." *IEEE Internet of Things Journal* 2, no. 2 (2015): 103-112.
[30] Jara, Antonio J., Alex C. Olivieri, Yann Bocchi, Markus Jung, Wolfgang Kastner, and Antonio F. Skarmeta. "Semantic web of things: an analysis of the application semantics for the IoT moving towards the iot convergence." *International Journal of Web and Grid Services* 10, no. 2-3 (2014): 244-272.
[31] Kocakulak, Mustafa, and Ismail Butun., “An overview of Wireless Sensor Networks towards internet of things”, *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1-6, 2017.
[32] Bhardwaj, Isha, Ajay Kumar, and Manu Bansal, “A review on lightweight cryptography algorithms for data security and authentication in IoTs”, In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 504-509, IEEE, 2017.
[33] Puthal, Deepak, Surya Nepal, Rajiv Ranjan, and Jinjun Chen, “Threats to networking cloud and edge datacenters in the Internet of Things”, *IEEE Cloud Computing* 3, no. 3 (2016): 64-71.
[34] Pongle, Pavan, and Gurunath Chavan, “A survey: Attacks on RPL and 6LoWPAN in IoT”, In *2015 International conference on pervasive computing (ICPC)*, pp. 1-6, IEEE, 2015.
[35] Zhou, Jun, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos. "Security and privacy for cloud-based IoT: Challenges." *IEEE Communications Magazine* 55, no. 1 (2017): 26-33.
[36] A. H. Adnan et al., “A comparative study of WLAN security protocols: WPA, WPA2,” *in Proc. International Conference on Advances inElectrical Engineering (ICAEE),* Dhaka, pp. 165-169, 2015.
[37] A. G. Sulaiman, and I. F. Al Shaikhli, “Comparative Study On 4G/LTE Cryptographic Algorithms Based On Different Factors,” *IJCST*, vol. 5, July 2014.
[38] Y. E. Gelogo, R. D. Caytiles, and B. Park, “Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security*,” International Journal of Control and Automation*, vol.4, no.4, pp.179-184, 2011.
[39] C. Hennebert, and J. D. Santos, “Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis,” *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 384-398, Oct. 2014.
[40] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” *Ad Hoc Networks*, vol. 11, pp. 2661- 2674, Nov. 2013.
[41] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, “SecKit: A Modelbased Security Toolkit for the Internet of Things,” *Computers & Security*, vol. 54, pp. 60-76, Oct. 2015.

[42] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe:Lightweight Secure CoAP for the Internet of Things,” *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711-3720, Oct. 2013.

[43] Brendel, Juergen, “World-wide-web server that finds optimal path by sending multiple syn+ ack packets to a single client”, U.S. Patent 6,587,438, issued July 1, 2003.

[44] Lu, Chenyang, Brian M. Blum, Tarek F. Abdelzaher, John A. Stankovic, and Tian He. RAP: A real-time communication architecture for large-scale wireless sensor networks. Virginia Univ Charlottesville Dept Of Computer Science, 2002.

[45] Mishra, Namrata, Shrabanee Swagatika, and Debabrata Singh, “An Intelligent Framework for Analysing Terrorism Actions Using Cloud”, In New Paradigm in Decision Science and Management, pp. 225-235, Springer, Singapore, 2020.