International Journal of Future Generation Communication and Networking
Vol. 12, No. 5, 2019 pp.173-185

# SECURITY THREATS IN IOT VIA LAYERED ARCHITECHTURE

Muzammil Hussain[1], Arshad Hashmi[2]
[1]*Department of ISE M V J College of Engineering Bangalore, India*
[2]*Department of Information Systems Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University Jeddah,* KSA

***Abstract***
*Internet of things (IoT) is an inventive innovation subject to all sorts of nonexistent and science anecdotal arrangements. Dreams and hypotheses are as yet conceivable about it. An innovation joining genuine items and virtual life (Internet) is to be sure a rich pitch of imagination and unique thoughts.. The Internet of Things (IoT) is a developing worldview concentrating on the association of gadgets, articles, or "things" to one another, to the Internet, and to clients. IoT innovation is foreseen to turn into a basic prerequisite in the advancement of savvy homes, smart grid, smart health, and smart gadgets as it offers comfort and proficiency to home inhabitants with the goal that they can accomplish better personal satisfaction. Use of the IoT model to savvy homes, smart health, smart gadgets by interfacing items to the Internet, presents new security and protection challenges as far as the classification, genuineness, and honesty of the information detected, gathered, and traded by the IoT objects. These difficulties make shrewd homes, shrewd health, and shrewd gadgets amazingly powerless against various kinds of security assaults, coming about in IoT-based brilliant homes being shaky. Hence, it is important to distinguish the conceivable security dangers to build up a total image of the security status. The purpose of this study is to identify security threats in IOT layers and provides solutions for each layer.*

***Keywords:*** *Security Issues, Integrity, MQTT, WSN, RFID, ISM and ECC.*

## I. Introduction

Kevin Ashton first suggested the “Internet of Things” known as an array of linked devices in 1998. It is a tremendous technological upset that has revived the present Internet base into an understanding of a considerably more powered figuring network where all the physical objects around us will be exceedingly visible and inescapably connected to each other [I]. IoT definitely has an enormous adaptability potential and promises an amazing future, yet it has a sequential power. There is some fluffiness about the Internet of Things theory, for instance, IoT can be divided into two Internet and Things pieces. The "stuff" are actual articles conveying EPC (Electronic Product Code)-like RFID tags. Omnipresent registration, which was thought to be a disturbing errand, has now become a reality due to advances in the field of programmed identification, remote correspondence, transmitted calculation procedure, and rapid Internet speed. Communication today is comprehensive as there is a growing enthusiasm for sharing information over the Internet. With a variety of explorations being carried out, IoT's dream is expected to become a reality soon [II]. As Gartner pointed out, around 25-50 billion extraordinarily recognizable articles are relying on being a piece of this worldwide figuring system constantly 2020, which is astonishingly a large number, anyway the commonality of such a huge system of interconnected gadgets will pose some new security and protection hazards and put each of these gadgets at a high risk for programmers as they are With the fast advancement of the IoT, variety of IoT applications is there that add to our daily existence on a regular basis. They spread from traditional hardware to objects of the general family unit, which help to improve the life of the human being. Improving IoT technology would genuinely jeopardize software vulnerability throughout the IoT system [II].In line with these lines, IoT needs assurance against hazards and vulnerabilities in order to achieve the fullest potential. Protection is defined as a method for ensuring an object against physical harm, unauthorized access, theft or disaster by holding the item's information highly classified and upright and rendering the item's data available at any level [III].

ISSN: 2233-7857 IJFGCN

The remaining structure of the paper has background with security issues, challenges and requirements in the following section, then the architecture of IOT with security issues protocols and solutions for each layer in section III. The section IV includes discussion and finally section V has the conclusion.

## II. Background

We are going to briefly describe in the following section regarding the important Security Issues, Challenges, and Requirements.

### Security Issues:

IoT is considered to be a revised version of various advances such as WSN (Wireless Sensor Networks), Mobile Broadband, and 2 G correspondence or 3 G interchanges Networks, so it is likely that IoT will be at the same risk that it is now a direct result of security imperfections.

- Each gadget connects to the Internet in IoT, which is not normally a safe domain. There are several persons out there who are equipped to deploy their code remotely for the various system splits.
- In IoT articles, converse with each other; along these lines, avoidance of protection and security can be possible.

This investigation is an examination of IoT security issues. The report defines the security needs and challenges that are routinely found in use by the IoT system. This further specifies the safety hazards and arrangements for each level of IoT layout making it increasingly stable and broad.

### Challenges:

There are following mentioned challenges faced by the Internet of Things represented in the table

| Interoperability | Resource constraints | Data volumes | Privacy Protection | Scalability | Autonomic control |
|---|---|---|---|---|---|

Table 1

**Interoperability:** Important security provisions should not prohibit the use of heterogeneous interconnected gadgets in the system coordinated by IoT [IV].

**Resource constraints:** Most hubs lack capacity limit, CPU and power in IoT design. For the most part, they use correspondence channels for low-data transfer capacity. Applying such safety techniques, such as recurrence bouncing correspondence and public-key encryption estimation, is now unacceptable. Under these conditions, arranging the security framework is uncomfortable [V].

**Data volumes**: Since some IoT systems utilize brief and unusual communication networks, there is a large number of IoT implementations, such as sensor-based, collaboration and enormous scale frameworks, which can require a large volume of dedicated network or database data. [V1].

**Privacy Protection:** Because a barely credible number of RFID frameworks lack adequate validation components, anyone can track labels and find out the personality of the articles that convey them. Information can be read by interlopers, but they can also change or even delete the content. [VII].
Scalability: The IoT system includes a huge number of hubs. The proposed IoT security component should be versatile [VIII].

**Autonomic Control:** Conventional PCs need consumers to model and adapt them to different application spaces and different situations for communication. However, questions in the IoT system should immediately build associations and sort themselves out / design to adjust to the stage in which work is being

done. Additionally, this type of control includes several systems and components, such as self-design, self-improvement, self-administration, self-recovery, and self-assurance [IV]

**Requirements:**

The important concern to apply security alleviation is to maintain and ensure users security in addition to data as well as the devices of IOT. Keeping this view following security requirements are mentioned in the table 2.

| Authenticity | Authorization | Confidentiality | Integrity | Availability and Continuity | Accountability |
|---|---|---|---|---|---|

Table 2

**Authenticity:** Entry to the computer or encrypted data is only permitted for legitimate users.

**Authorization**: The benefits of device categories and apps should be limited as they can only get to the capital, they have to make their errors.

**Confidentiality**: Sender-receiver communication should be protected from intrusion by strangers.

**Integrity**: The information/data received during communication should not be changed from sending to the receiver.

**Availability and continuity:** In order to avoid possible organizational disappointments and interferences, it is important to guarantee transparency and continuity in the arrangement of protection authorities.

**Accountability**: The data received will show that it came from the legitimate user.

**III. Architecture of IOT with Security Issues Protocols and Solutions for each Layer:**

IoT devices are flexible to connect to the Internet and automatically reconfigures. Thus, due to flexibility 2 types, IOT architecture is defined.

1) Three-Layer Architecture with security threats.
2) Five -Layer Architecture with security threats

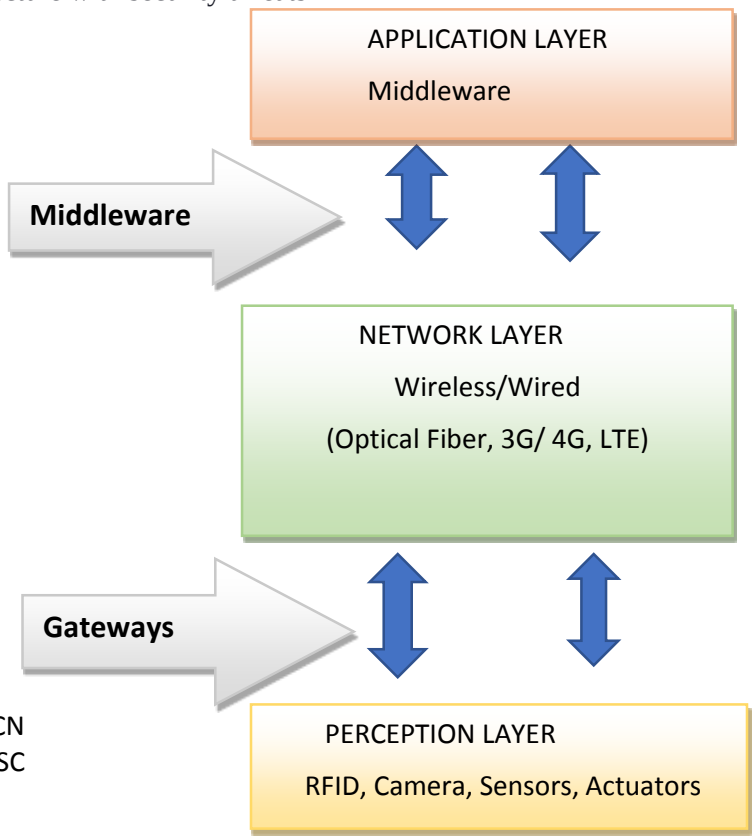

Fig 1. Three-Layer Architecture with security threats

**3-Layer Architecture:**
The Three-layer architecture in figure: 1 contains perception layer, network layer and application layer. We are going to discuss each one in brief in the following section.
**Perception Layer:** This layer gathers environmental data. Sensors, actuators, and RFID are used in this layer of camera. This layer is used to distinguish articles and collect target data, and the key advances of this layer are RFID labels, cameras, sensors, actuators, changing the data into digital signals. This layer's software is affected by vitality and energy. At the same time, in a threatening situation, a sensor gadget can operate and can be effectively decimated. This has a strong impact on the entire framework's expertise. [IX].

**Security issues in the layer of perception:**
Construction level is the smallest IoT. The perception layer is the basis of IoT-wide access to information. The issues in the Perception layer consist of sensing system physical protection and information collection security. IoT cannot provide a safety protection system and is weak to attack because of heterogeneity, restricted power, easy and poor sensing node protecting functionality which affects, RFID and M2 M terminal privacy. The RFID includes safety issues like leakage of information, tracking of information, manipulation and man-in-the-middle attacks. The awareness layer security issues include physical capture, unequal attacks, latency assault, network cloning attack, and forward attack. Now we will briefly discuss the protocols in perception layer.

**Protocols in perception Layer:** It consists of Bluetooth Low Energy (BLE), Z-Wave, ZigBee Wave, DASH7, LTE and LoRaWAN.
**BLE:**
This energy is a commonly used short-term communication standard for a layer of data link in IoT. It is mostly used for networking in cars. It has a slight delay 15 times lower than Bluetooth's initial requirements. The low energy can be 10 times less as compared to conventional.

**Bluetooth:**
This access control utilizes a low latency and fast transmission MAC without contention. This adopts a structure of master and provides two forms of frames: ads along with information frames. The advertisement frame used to experiment along with one or more specific marketing platforms is sent by slaves. Master nodes feel channels of ads to locate and bind slaves. The master informs the slave that it is a waking process and schedules series after contact. Normally nodes are up only when they talk and otherwise go to sleep to save their energy [X-XI].

**Z-Wave:**
Z-Wave is a low-energy MAC protocol developed for home automation but increasingly utilizes in many Internet of things implementations, including elegant homes and small business domains. This spans a range of up to 30 meters, point-to-point contact, and can be used for short communications. In contrast to limited ACK texts, it utilizes CSMA / CA for media access for the efficient programme. It reflects a master model in which the owner manages the slaves, gives them instructions as well as schedules the entire network [X].

**ZigBee Smart Energy:**
Out of all ZigBee is that the most ordinarily enforced IoT protocols for remote controls, and health care systems for a medium-range property. The topologies for networking embody circles, groups, or clusters

in very network topology, the core of tree topology and anyplace in a peer-to-peer topology, a supervisor manages the network and is positioned at the center. The ZigBee generic describes 2 stack types: ZigBee and ZigBee professional. These stack profiles hold complete mesh networking conjointly operating with numerous applications permitting the implementation of low memory moreover process power. ZigBee professional offers further capabilities likewise as exchange security, random address assignment quantifiability and improved dependableness with economical multi-to - one routing mechanisms [XII]

**DASH7:**
It is the latest without wire networking standard which works in the worldwide available industrial science medical (ISM) band of functional RFID phones. It is planned primarily for flexible, long-range outdoor protection with a high data rate in comparison with standard ZigBee. IPv6 addressing is being supported by low-cost solutions as well as encryption. This follows a slave design and is considered as a pulse transitive traffic as well as considered ideal for IoT [XIII].

**Filtering:**
Three processes filter are considered in an incoming frame: cyclic redundancy check, a four-bitt subnet mask, as well as an evaluation of the quality of the link. It can be processed if the frame passes those checks, but otherwise, it won't.

**Addressing:**
Two kinds of addresses are being used there; the exceptional identifier that is the EUI-64 ID as well as the dynamic network identifier that is a network administrator-specified 16-bit address.

**Frame format:**
A fixed-size MAC frame with a maximum capacity of 255 bytes, including encoding, subnet, approximate transmitting power, and some other optional fields.

**LTE-A:**
Such networks to satisfy money supply M and IoT necessities. Among different cellular protocols, this is often the foremost scalable and value-effective standards. LTE-A was free in twenty-one centaury with many updates to support new technology on an associate in progress basis. Historically, it uses multiple access orthogonal frequency division as a medium access technology wherever the frequency is differentiating into numerous subcarriers. LTE-A's structure is created of a core and radio access network likewise as remote nodes. The core network is answerable of observance mobile devices and recording their IPs. RAN is putting in place control and information planes and managing wireless property and control of radio access. RAN and CN communicate via the S1 association, wherever RAN is that the eNB to that different mobile nodes are wirelessly connected [XIV]. In distinction, LTE-A's new releases (LTE Rel-13 and Rel-1) [XV]. Rel-13 introduced three main features: FD-MIMO, accrued aggregation of spectrum beside carrier, conjointly new machine-type commination services. Multiple output Full Dimension Multiple Input needs to boost spectrum potency by mistreatment numerous base station antenna ports. Compared to the already used approved radio bands, the utilization of recent frequency assets is achieved by mistreatment unauthorized spectrum. During this approach, a lot of ranges are used and continuity with existing devices is preserved backward. Increasing the height rate and optimum allocation of frequency assets have conjointly been wont to boost the convergence of networks in LTEA. In distinction, LTE-A Rel-13 provided new machine-type communication services together with a price reduction, swollen vary help, indoor routing, and single-cell distributed and multicast access. With a lot of antenna passage, economical communication, and reduced input, the LTE Rel-14 design is meant to any improve FD-MIMO. However, the discharge is meant to standardize the reduction of latency, vehicle to something likewise as downlink multi-user communication self-addressed as feasibleness studies.

**LoRaWAN:**
It is a recently made wide-area long-range wireless network architecture intended for IoT implementations with power savings, low cost, flexibility, safety, and bidirectional communication specifications. Multi-million-device flexible wireless networks are being designed by a low power usage integrated framework. This embraces scalable service, location-free, low power, and energy harvesting technology to meet IoT's future wants while promoting flexibility along with user-friendliness. [XVI].

**Security Solutions for Perception Layer:**
Long times until IoT, the discernment level security measures were taken back. Gear's, for instance, include successful confirmation for RFID, GPS, pathways, detectors, and other gadgets. Poor physical protection has been listed by OWASP in the top 10 IoT flaws. They need to ensure that the licensed persons will access the delicate data generated by devices or physical objects as a matter of primary importance. In order to do this, we need to define the visual character techniques and navigate the table. Comparatively, IoT must fulfill the approval procedure and validation procedure and its needs. Sorting of data in this layer is a major issue. Many suggested security systems, such as sight and sound stress encoding, water verification, stenography, authorized invention and time session, can be used for sight and sound data. Cryptographic handling is one of the fundamental assignments in verifying the sensor information on IoT for picture information assortment picture pressure and the Cyclic Redundancy Check can be used to verify images. Such activities include authentication and unscrambling, the era of key and hash, and the signature and testing for hashes widely used in applications to guarantee information security. Researchers has found two topsy-turvy Elliptic Curve Cryptography (ECC) and RSA calculations on sensor hubs and show that ECC efficiency is more notable than RSA and hilter kilter cryptography is suitable for asset controlled equipment. In this way, analysts focus on reducing the unpredictability of unbalanced cryptographic calculations and key conventions of dissemination. Such kinds of inquiries and enhancements make cryptographic devices slowly ideal for remote sensor arrangements in a unique circumstance. While extraordinary updated plans are being made, there is still no institutionalized plan to upgrade the administrations at the same time. Hazard Analysis is a basic component of the Internet of Things safety which measures the magnitude of the threat and the dangers related to the IoT environment. There are various recommendations that multiple organizations have produced to direct the identification of hazards, the International Standards Organization; and the International Electro technical Commission.Now we will briefly discuss the second consecutive part network layer of this architecture in the following section.

**Network Layer:**
The layer is accountable for the IoT infrastructure's availability. It also collects and transmits information from the layer of perception to the upper layer. The transmission medium could be wired or wireless, and the main advances are ZigBee, Bluetooth, 3G, and 4G. Network layer assaults are diverse, typically affect work coordination and data sharing between gadgets. [XVII].

**Security issues in network layer:**
The Internet of Things poses certain network threats such as unauthorized entry, privacy, eavesdropping of information, honesty, DoS attacks, disruption, man-in-the-middle attack, and many others. IoT sensing many devices contribute to a multitude of data collection types along with data knowledge that includes huge, multi-source and heterogeneous functionality. It will also cause network security issues such as the need for various nodes to transfer data, leads to a set of connections congestion, leading to DoS attacks.
The network layer separates data transfer from experience level to application layer into two protocols. The routing layer moves packets from origin to destination and the packet is generated by the encapsulation layer. Now we briefly discuss network layer protocols.

**Network layer protocols:**

It mainly consists of routing and encapsulation. We will discuss summarized points of each related protocols.
First we will elaborate in brief the routing network protocols which consists of RPL (routing protocol for Low Power), CORPL, CARP (channel-aware routing protocol) and E-CARP.

**RPL:**
The routing protocol for Low Power beside Loss Network (LPL) could be a distance-vector protocol developed at IETF for IoT application routing. It supports all of the higher than mentioned waterproof layer protocols and a few different non-IoT protocols. It also supported directed-acyclic (DODAG) graphs with just one path from each leaf node to the basis throughout that all leaf node traffic is redirected. Originally, the node can apply a DODAG object of knowledge (DIO) advertising itself because of the heart. Once DIO sent, propagated to the guts, a target advert object (DAO) is distributed to its oldsters from the node and supported the destination, the supply determines wherever to route. New nodes can submit the associate application to achieve the DODAG info Request (DIS). RPL nodes, the foremost standard or unsettled nodes are often unsettled [XVIII].

**CORPL:**
It has the capability to extend RPL by virtue of DODAG-like technology. First, this implements expedient forwarding that permits many forwarders to be designed by the packet, however solely the strongest next hop to forward the packet are elect. Then each node creates solely a forwarding list in its place of a parent and updates its neighbor. On the idea of updated info, each node updates its neighboring priorities dynamically to form the forwarders array [XIX].

**CARP and E-CARP**:
The channel-aware routing protocol (CARP) is another naming developed for underwater communication, focused on decentralized networks. It is a lightweight protocol for packet communication and can, therefore, be extended in IoT applications. This uses historical calculations of the reliability of the connection to determine the route of transmission. Initialization of the network and transmission of data are the 2 scenarios that are measured in these protocols. A HELLO packet is broadcast between the sink and other nodes in the networks in network initialization. In data transmission, the packet is routed in a hop-by-hop fashion from the sensor to the sink. Each next jump is autonomously decided. The main issue with CARP is that the reusability of earlier collected data is not supported. For instance, if the application only wants sensor data when it significantly changes, then the transmission of CARP data is not useful to that particular application. Throughout E-CARP, an extension to CARP was rendered by enabling the sink node to save sensory data previously received. E-CARP sends a ping packet when new data is requested. Thus, E-CARP dramatically declines overhead communication [XX].Now we will discuss the second important part of the routing protocol named as encapsulation.

**Encapsulation:**
It mainly includes three important components 6LowPAN, 6TISCH and 6Lo. These three will be described in brief in the following section.

**6LowPAN:**
One of the primary and wide used IETF standards during this class is that the IPv6 over low-power wireless personal space network (6LoWPAN). This basically encapsulates giant headers of IPv6 in little waterproof frames of IEEE802.15.4, which may not surpass the scale of 128 bytes. 6LoWPAN standards offer several characteristics including numerous hierarchal addresses, dissimilar network topologies, low latency, efficient, versatile networks, flexibility, consistency and drawn-out sleep times. Within the standards, header compression is employed to reduce overhead transmission. Frames in 6LoWPAN use four header

types: header 6loWPAN (00), header dispatch (01), header mesh (10). Any frame that doesn't meet 6loWPAN specifications is discarded in header case No 6loWPAN. The dispatch header is employed for compressions of headers for multicasting and IPv6. For broadcasting, mesh headers are used; whereas fragmentation headers are wont to break long headers of IPv6 to suit into fragments of 128 bytes.

**6TiSCH:**
It could be a totally different 6TiSCH unit IETF commonplace. It defines forms within which IEEE 802.15.4e information links can transfer long IPv6 headers via TSCH mode. The usable frequencies and their time slots are hold on during this mode in a very matrix named the utilization matrix for channel management. This matrix is split into numerous chunks containing time and frequencies in every chunk, likewise as all nodes within the network are thought of globally. Nodes coordinate and discuss their programming among an equivalent interference domain so they'll all transmit while not an interruption. Optimization downside could be programming wherever one or two of neighbor nodes sharing a similar application are allotted to time slots. The specification doesn't specify however designing are often disbursed associated leaves it as an application-specific issue of optimum flexibility of varied IoT applications. The arrangements are often clustered or unfold in conjunction with the package or topology utilized in the waterproof layer [XXI].

**6Lo:**
A recently named IETF cluster called IPv6 over resource-constrained node networks (6Lo) is that specialize in implementing a series of IPv6 frame transport necessities across numerous information links. Despite the event of 6LowPAN beside 6TiSCH for encapsulation functions, it became apprehensible that a lot of principles are needed to hide all standards for information links. For this purpose, 6Lo was fashioned by IEFT. Most of the 6Lo necessities weren't completed at the time of this writing and are in numerous drafts phases. 2 of the "IPv6 over G.9959" associated "IPv6 over Bluetooth Low Energy" 6Lo specifications are approved as an RFC.

**Security solution for network layer:**
System layer security can be assessed in two remote and wired primary sub-layers. One of the underlying activities in remote security sub-layer is the improvement of confirmation conventions and key administration. For example, IP protection convention (IPSec) is created to verify the layer of the network and SSL / TLS is created to protect the link in the layer of the device. In each sheet, they offer identification, integrity, and fairness. By using PPSK (Private Pre-Shared Key) for each system-related device or detector, the IoT platform provides an additional security mechanism. The entrance room for each form of the gadget can be efficiently defined by having excellent special keys. Besides, disabling default passwords and visitors in system gadgets, such as switches and outputs, should be performed promptly after another system gadget has been created. This includes the board's secret phrase, solid approaches to secret phrases, and occasional password changes.The wired sub-layer security is worried about the gadgets that use wired media in the IoT framework to talk to each other. Some regular security strategies used in wired systems are, what's more, the Intrusion Prevention System (IPS) firewalls. If a device is unlikely to have an IPS or firewall, it can closely test the arrangement of bundles that are goal-oriented. Existing IoT platform, though, cannot sift parcels and analyze packets. There are inquiries about this issue where security analysts try to build a low asset hungry IoT firewall that enables bundle evaluation. Now in the following section we will briefly discuss the topmost application layer of this architecture

**Application Layer:**
The software layer is the Internet-of-Things social division, consolidating with the market question and defining specific intellectualization. Its framework operates different applications in different situations.

Used to track and process information from the middleware level, this layer also includes the last client's performance support [IX]. The problem of use surface arises mainly in the processing of sensitive information, like unauthorized access to information, unfavorable changes of information and the period of consent [XVII]. Assailants may attempt to assault frameworks with code vulnerabilities to increase and adjust touchy information.

**Security issues in the application layer:**

IoT implementation is the product of near integration of communication technology, computer technology and technical business that can see implementations in many forms. In the application layer, security issues include eavesdropping and manipulation [VIII]. Its framework carries out traffic management duty. It also provides tools for various applications that conduct data conversion into a comprehensible type or by submitting queries [V] helps in information collection. In the application layer, a path-based DoS attack initiates by stimulating the sensor nodes creating vast traffic on the way to the base station. Few important application layer protocols will be described in the following section.

**Application layer protocols:**

It consists of mainly five protocols which we are going to discuss in brief in the following section.

**Constrained Application Protocol (CoAP):**

It was used for low-power as well as low-memory built-in devices where it could be utilized for communication in its place of HTTP. HTTP protocol with the request/response paradigm is currently available, but HTTP has a lot of features and more footprints [XXII]. HTTP runs over TCP where TCP's three-way handshake and many more dynamic processes would take more time. There's no need for this strong protocol now for low-power embedded devices and we can simplify it to operate over TCP. As CoAP is a web transfer protocol that can be used with restricted networks. CoAP uses the same method template client / server as HTTP [XXIII].

**MQTT (Message Queue Telemetry Transport):**

It was developed by IBM in the late 20th century and standardized by OASIS in the early 21st century to attain lightweight M2 M interaction**.** It is similar to client/server protocol architecture publish/subscribe. Due to its simplicity, the significance of the MQTT protocol is because of a lack of high CPU and memory usage (the reason is the lightweight protocol) [XXIV]. MQTT embraces a wide range of mobile platforms and phones. TLS / SSL protection is given to MQTT on the transport layer.

**Extensible Communications and Presence Protocol (XMPP):**

It is a communications protocol originally planned to communicate along with exchange messages. It was developed over a decade ago by the IETF. Only XMPP protocol supports publish/subscribe and request/response framework in all application layer protocols, and it is up to application developers to establish the template they are using [XXV]. This does not assure service quality and is therefore not realistic for M2 M communications. XMPP is seldom utilizing in the Internet of things, but it has developed some interest in improving its technology to benefit IoT applications.

**The Advanced Message Queuing Protocol (AMQP):**

It is a protocol that operates across the economic sector. Use TLS / SSL protocols, protection is controlled. It's operating over TCP. AMQT follows the message protocol to publish/subscribe [XXVI]. AMQP is the same as MQTT, but AMQT then forward it to its store data, and this feature used when disrupting the network ensures reliability. A broker divides it into two parts of the exchange and queue. Exchange liability for receiving messages from publishers and for delivering to the list. Queues are based on pre-defined roles also conditions and are generally sent to subscribers who subscribe to these data

**Web-Socket:**
It provides two ways to communicate with a remote server between clients. Web-Socket provides similar security to the HTTPS protocol used in the security model. Using the application layer and web-socket operate on TCP transport layer protocol for surfing, so those communicating to remote need to link and communicate with the host. Web-Socket is a web-based protocol that runs on a single TCP stream, providing full-duplex communications. Web-socket session starts without publishing / subscribing and request/response templates such as previous protocols [XXVII].

**Security Solution for Application Layer Protocol:**
This comprises of two important sub-layers. There are neighborhood programs and associated middleware functionality in the first sub-layer that should be tested for various systems. For example, methods of cryptography can be used in intelligent transport frameworks, whereas methods of steganography are used in informative home / canny metering frameworks. After national uses and their protection mechanisms, the subsequent layer takes over which ensures the safety of the data sent and obtained. Henceforth, in these systems, different security protocols are implemented depending on the degree of each system, such as validation, authorization, check to list, precise reporting, place of intrusion, firewall, and antivirus. The most important things is the gatecrashers [VII] are anticipated by a confirmation strategy that is useful in the help layer and fused independence that distinguishes the evidence from the application layer. The methodology of safety identity is the same as in the company layer. The main distinction is that, with the help of some coordinating administrations, they focus on validation. The client can now select the data that they need to pass on to these administrations. Information security is one of these layers ' problems. This can be resolved by security framework using

- Anti-infection programming and safe programming testing against administrative escape clauses and antagonistic code infusion, an assortment of well-being measures are taken on IoT.
- Temporary store improvement and confirmation of information against antagonistic tasks
- Session check techniques to stop assaults like re-try session and capturing
- Boundary check, asset get to control and information encryption techniques to avoid protection spillage.

The IoT is vulnerable against numerous attacks as previously portrayed. Interruption detection is now a basic idea of IoT set up in this world such as mechanization of systems, savvy lattices, genius metering, and robotic robotization. A security instrument widely referred to as IDS (Interruption Discovery Framework) distinguishes assaults during activity review against a framework. Once the attack has been detected, it reports the information or IDS records for an alert. There are various techniques to detect interruptions, such as data extraction process, anomaly detection technique, observable inquiry, and so on. This completes the brief discussion related to 3-Layer architecture, security issues and their related solution. Now in the following section we are going to discuss the 5-Layer architecture, security concern and its remedy.

**5-Layer Architecture**:

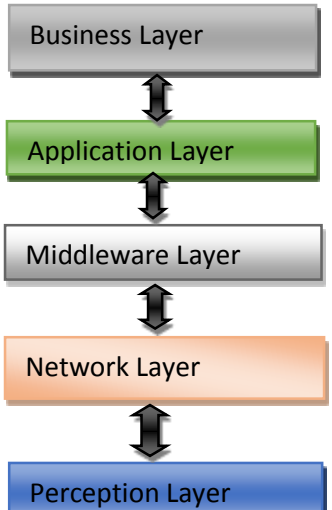

Fig 2. Five Layer Architecture

The fig 2 represents the 5-Layer architecture of IOT. The 5-Layer Architecture in Internet of Things comprises on the following layers as mentioned in table 3.

| Perception Layer | Network Layer | Middleware Layer | Application Layer | Business Layer |
|---|---|---|---|---|

Table 3

In this 5-Layer architecture three layers are same with respect to the 3-Layer architecture. So we are going to discuss only two additional layer Middleware and Business layer.

**Middleware Layer:**

This layer receives information from the network layer, connects the framework to the cloud as well as database, and executes handling and capacity of information. Because of the rapid advancement of distributed computing and IoT, the middleware layer be able to give the more predominant capacity and processing capabilities. Each layer instead provides APIs to satisfy the software layer's demands. Database protection and network safety are the key issues that affect the essence of operation in the application layer in the middleware framework.

**Business Layer:**

This layer deals with the general administration and exercises of the IoT framework. Business Layer builds a business model, graphs, and flowcharts, based on Application Layer's data. The Business Layer also conducts, schedules, monitors, dissects and constructs IoT defined modules. This layer underpins choice processes that are based on Big Data analysis. Furthermore, Business Level monitors and works with the essential four levels. It also contrasts each layer's yield and anticipates that yield is expected to improve administration. It produces distinctive action plans for successful business processes [XXVIII]. The following section will have the brief discussion of this study.

## IV. Discussion

The finding of this study clearly shows that Internet of Things (IoT) is an environment through an object is connected to the Internet through edge devices. These edge devices having layered architecture and protocols to flow the data between user and system. Since the data to and fro takes place between different objects and devices there is need of security measure to protect the user and device communication as well as the seamless connection would be provided between the users.

We highlighted three and five layers architecture. The most commonly used architecture is three layer. In the layer we studied security threat, protocols and solutions. In short Internet of Things (IoT) security is essential and need more attention to resolve the security issues which can protect data.

## V. Conclusion

For cybercriminals, IOT is an easy target. We illustrated the insecurity of protection across various layers in this article. Each layer has its own components and threats to security. The modules must use proper security fixes to prevent security breaches from each level. IoT is another and growing innovation that has attracted considerable attention from around the globe. Because of the assist of some major commitments, this innovation has become versatile in our day-to-day lives. Nonetheless, certain fundamental issues of

this new innovation seem to be security concerns, and they need more effort to be dealt with properly and to complete this invention. A troubling image was created by our analysis of some smart gadgets. Notwithstanding a virtually steady stream of intrusion event media reports and electronic attacks, there are still multiple devices that are not using encrypted communications or effective authentication techniques. In this article, IoT's major security concepts have been extensively discussed and analyzed. It collected and studied the problems it posed and its numerous prerequisites and was separated under different headings. A wide range of safety hazards in the area of IoT, which may become a barrier during its implementation or when its development has been investigated and organized as specific application levels of IoT infrastructure, network level, awareness layer.

**References**

[I] Knud Lasse Lueth, "IOT basics: Getting started with Internet of Things". March 2015, http://www.iot-analytics.com.

[II]Aaditya Jain, Bhuwnesh Sharma, Pawan Gupta,"INTERNET OF THINGS: ARCHITECTURE, SECURITY GOALS, AND CHALLENGES- A SURVEY" in International Journal of Innovative Research in Science and Engineering, Vol. No. 2, Issue 04, April 2016.

[III] J. M. Kizza, "Guide to Computer Network Security"2nd Edition,ISBN: 978-1-4471-4543-1 Springer, 2013.

[IV] ITU-T. Y.2060: Overview of the Internet of Things,http://www.itu.int/rec/T-REC-Y.2060-201206-I

[V] Arseni, S.C., Halunga, S., Fratu, O., Vulpe, A. and Suciu, G." Analysis of the Security Solutions Implemented in Current Internet of Things Platforms". IEEE Grid, Cloud & High Performance Computing in Science Romania, conference 28-30 October 2015,PP.1-4.

[VI] Mattern, F. and Floerkemeier, C. (2010) ,"From the Internet of Computers to the Internet of Things." , Springer, Berlin Heidelberg, pp.242-259.

[VII] 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 issue-7, pp.1-6.Fab,2015.

[VIII] Nguyen, K.T., Laurent, M. and Oualha, N. ," Survey on Secure Communication Protocols for the Internet of Things." Ad-Hoc Networks, 32, pp,17-31,September,2015.

[IX] Pateriya R, Sharma S ," The evolution of RFID security and privacy: a research survey", In 2011 International Conference on Communication Systems and Network Technologies (CSNT). IEEE, pp 115–119, July, 2011.

[X] J. Decuir, "Bluetooth 4.0: Low Energy," 2010, https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf , (accessed February 24, 2017).[XI]C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology," In Sensors, vol. 12, issue, 9, pp. 11734-11753,Aug 2012.

[XII]Zigbee,"Zigbee resource guide,"October, 2016, http://www.nxtbook.com/nxtbooks/webcom/zigbee_rg2016/#/0, (accessed February 24,2017).

[XIII]O.Cetinkaya and O.Akan, "A dash7-based power metering system," in 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pp,406–411, Jan, 2015.

[XIV] J. Lee, Y. Kim, Y. Kwak, J. Zhang, A. Papasakellariou, T. Novlan, C. Sun and Y. Li, "LTE-advanced in 3GPP Rel -13/14: an evolution toward 5G," in IEEE Communications Magazine, vol. 54, no. 3, 2016, pp. 36-42.

[XV]C. Hoymann, D. Astely, M. Stattin, G. Wikstrom, J. F. Cheng, A. Hoglund, M. Frenne, R. Blasco, J. Huschke and F. Gunnarsson, "LTE release 14 outlook," in IEEE Communications Magazine, vol. 54, no. 6, 2016, pp. 44-49.

[XVI]N. Sornin, M. Luis, T. Eirich, T. Kramp, and O.Hersent, "Lorawan specification," LoRa Alliance, January 2015,

https://www.loraallianceorg/portals/0/specs/LoRaWAN%20Specification%201R0.pdf, (accessed February 24, 2017).

[XVII] Zhang W, Qu B ,"Security architecture of the Internet of Things oriented to perceptual layer", Int J Comput, Consumer Control (IJ3C), Vol2,Issue,2:pp37–45,2013.

[XVIII]T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, March 2012.

[XIX]Aijaz and A. Aghvami, "Cognitive machine-to-machine communications for internet-of-things: A protocol stack perspective," in IEEE Internet of Things Journal, vol. 2, no. 2, 2015, pp. 103-112.

[XX]S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "Carp: A channel-aware routing protocol for underwater acoustic wireless networks," in Ad Hoc Networks, vol. 34, 2015, pp. 92-104.

[XXI]D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6tisch: deterministic ip-enabled industrial internet of things," in IEEE Communications Magazine, vol. 52, issue ,12, 2014, pp. 36–41.

[XXII] Internet Engineering Task Force, "IPv6 over Networks of Resource-constrained Nodes (6lo)," https://datatracker.ietf.org/wg/6lo/documents/, (accessed February 24, 2017).

[XXIII] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things:A survey on enabling technologies,protocols and applications," in IEEE Communications Surveys Tutorials, vol. 17, no. 4, 2015, pp. 2347-2376.

[XXIV] IEEE802.15.4-2011, "IEEE standard for local and metropolitan area network–part 15.4: Low-rate wireless personal area networks (LR-WPAN)," in IEEE Standards, April, 2012, pp.1-225.

[XXV] M. Park, "IEEE 802.11ah: sub-1-ghz license-exempt operation for the internet of things," IEEE Communications Magazine, vol.53, no. 9, 2015, pp. 145-151.

[XXVI] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash ―Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications‖ ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.

[XXVII] Ding Z-h, Li J-t, Feng B (2008) A taxonomy model of RFID security threats. In: 2008 11th IEEE International Conference on Communication Technology. ICCT 2008. IEEE, pp 765–768.

[XXVIII]Khoo B (2011) RFID as an enabler of the Internet of Things: issues of security and privacy. In: 2011 International Conference on Internet of Things (ithings/CPSCom) and 4th International Conference on Cyber, Physical and Social Computing. IEEE, pp 709–712.