A Review on IoT: Layered Architecture, Security Issues and Protocols

Tooba Rashid[1†] **and Sumbal Mustafa**[2††]

University of Lahore, Gujrat Campus, Pakistan

Summary
The Internet of Things (IoT) is the most creative and focused technology to be employed today. It increases the living conditions of both individuals and society. IoT offers the ability to recognize and incorporate physical devices across the globe through a single network by connecting different devices by using various technologies. As part of IoTs, significant questions are posed about access to computer and user privacy-related personal details. This article demonstrates the three-layer architecture composed of the sensor, routing, and implementation layer, respectively, by highlighting the security risks that can occur in various layers of an IoT architecture. The article also involves countermeasures and a convenient comparative analysis by discussing major attacks spanning from detectors to application. Furthermore, it deals with the basic protocols needed for IoT to establish a reliable connection between objects and items.

Keywords:
IoT, architecture, security attacks, countermeasures, protocols.

1. Introduction

Now-a-days, the Internet has become a basic need. People are communicating and sharing information through the internet. Different communication technologies are used to exchange information. In 1999 the word "Internet of Things" was first used in supply chain management by Kevin Ashton. "Iot" refers to a modern world where all machines are connected through the internet and can be used collectively to efficiently conduct some challenging tasks. The number of IoT apps increases every day. It is estimated that the number of "IoT" systems has more than increased since 2012 and that there will be 50 billion systems running on the World wide web [1]. This "IoT" term consists of several devices that can be wired or wirelessly attached to one another; all machines are heterogeneous in type. The purpose of "IOT" is that devices can connect easily. Internet communication is possible due to new technologies, such as RFID, WSN, and IPv6. The "RFID" allows labeling or marking of each system as the main identification tool in the "IoT" Each "thing," i.e., people, machines, etc., becomes a wireless entity due to "WSN" and can communicate between the cyber, physical, and digital worlds [2]. "IoT" links the world via physical devices that are integrated with various kinds of sensors. It offers many benefits such as a sensor system with a communication network, storing and managing information, providing access, but on the other hand, it poses some problems such as data privacy, availability, and security. The issue we have to focus on is data privacy and security. We need to ensure the strong encryption that our data is completely secure with complete protection. Many vulnerabilities on "IoT" infrastructures emerged because of no data exchange encryption system, poor passwords, insecure data sharing platforms, and data exposure. If the "IOT" systems are improperly protected, they can be used as a gateway by cyber hackers to damage other systems on the network [3]. This problem requires a well-defined security infrastructure that can evaluate these issues and minimize security threats. Process to secure any entity from physical damage, loss or theft, untrusted access by maintaining high data integrity and high secrecy with respect to the entity[4]. The method of recognizing system threats and system vulnerabilities are needed to specify a reliable, wide set of security requirements and also helps determine whether the security method is appropriate safe from malicious attacks [5]. The layered architecture is the best way to explain IoT, and usually "IoT" consists of three-layered architecture. The core layers are the implementation layer, routing layer, and the sensing layer. We need to build a secure transmission of data by considering the IoT architecture. We face various kinds of attacks from external as well as internal devices on different layers.

The content of this paper is set out as follows: Section 2 provides information about literature. Section 3 discusses IoT three-layered architecture. Section 4 provides an overview of security attacks associated to each layer. Section 5 provides countermeasures and analysis of attacks on the basis of different matrices. Section 6 discusses basic protocols which are necessary for reliable communication, Section 7 discusses the performance discussion and Finally, Section 8 describes the conclusion of the review .

2. Related Work

To figure out the current problems and the solution that has already been viewed, we are studying some papers

Manuscript received September 5, 2023
Manuscript revised September 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.9.13

that are already issued. This provides us an understanding of the attacks we face and how they affect the IoT world.

Table 1

Sr. No	*Paper Name*	*Author and Year*	*Contribution's*
1.	A survey on internet of things: Security and privacy issues.	J. Sathish Kumar, Dhiren R. Patel, 2014	In this paper, they assessed security and privacy issues at various layers. It introduces an array of new issues about privacy infringement and the protection of information. This approach combines computer protection with business implementation and node communication [6].
2.	Secure layers based architecture for Internet of Things.	Dhananjay Singh, Gaurav Tripathi, Antonio Jara, 2015	The layered foundation architecture for IoT system is discussed in this document. We access remote location devices through some system interface, so the essential need for IoT is protection. The layers divided into five sections that render IoT easy to handle [7].
3.	IoT: A review on security issues and measures.	Ravindran, R., J. Yomas, and E. Jubin Sebastian, 2015	The Researcher focuses on different security measures. To provide the RFID authentication, physical measures or code methods, or a variety of both mechanisms are used. It is essential that trusted different kinds of intelligent sensor technology [8].
4.	ARMOUR: Large-scale experiments for IoT security & trust.	Salvador Pérez ,Juan A. Martínez, Antonio F. Skarmeta ,Márcio Mateus, Bruno Almeida ,Pedro Maló, 2016	To have some calculation of protection to assess such risks on the “OneM2M discus”. Explore the remote health plan and the smart cities [9].
5.	IoT architecture challenges and issues: Lack of standardization. Technologie.	Sarah A. Al-Qaseemi , Hajer A. Almulhim , Maria F. Almulhim , Saqib Rasool Chaudhry, 2016	This paper explores issues relating to the absence of standardizing, difficulties as well as the study of existing state-of-the-art requirements to illustrate and address it by proposing some technological solutions by proposing Microsoft Azure and smart things respectively. Internet of things development and IoT stability was negatively impacted by a lack of localization [10].
6.	Security threats and issues in automation IoT.	Pal Varga; Sandor Plosz; Gabor Soos; Csaba Hegedus, 2017	This paper explores the potential threats that may occur in multiple layers of an IoT infrastructure, particularly in the domain of automation. This study assembled and outlined potential risks of the internet of things automated systems in a layered approach. We find that there are drawbacks of WSN nodes used in the internet of things that can't be resolved explicitly because of the simplicity of such systems only in higher layers [11].
7.	Internet of Things (IoT): A vision, architectural elements, and security issues.	Shivangi Vashi; Jyotsnamayee Ram; Janit Modi; Saurav Verma; Chetana Prakash, 2017	In this article, we have an outline of the IoT architecture with the assistance of a Smart Environment. To overcome these protections of IoT devices, solid encryption and verification are required. This paper clarified the security issues in each layer and its estimates, which help us to comprehend and to improve security in IoT design. More intelligent security frameworks that managed risk recognition, error detection, and predictive investigation need to advance [12].
8.	Cyber security—IoT	Swapnil Naik ; Vikas Maral, 2017	To avoid system clone attacks, the system authentication mechanism is provided the link in which we need to insert another 8 bytes of encoded secession key when the system posts data on the server [13].
9.	Evaluating critical security issues of the IoT world: Present and future challenges.	Mario Frustaci, Pasquale Pace, Gianluca Aloi, Giancarlo Fortino, 2017	In each layer of IoT, certain security threats are protected, and the more user-friendly layer of IoT is the sensing/perception layer due to heterogeneous applications. Some lightweight methods must, therefore, be applied to this layer [14].
10.	Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures.	Uwazi Emmanuel Chinanu* & Onoja Emmanuel Oche & Joy O. Okah-Edemoh, 2018	This document proposes some important security techniques such as encryption to protect "IoT" apps and shared data through the IoT system. "IoT" encircles and links the environment via physical objects equipped with various sensor forms, which can be [15].
11.	Security challenges facing IoT layers and its protective measures.	Tariq Aziz Rao, Ehsan-ul-Haq, 2018	This document proposes the safety steps that will improve the "IoT's" efficiency and reliability. In order to enhance the security precautions in the IoT system, it is necessary to build new lightweight cryptographic algorithms and key management strategies that require the lowest processing power [16].
12.	Assessing risks and threats with layered approach to Internet of Things security.	Murat Aydos, Yılmaz Vural, Adem Tekerek, 2019	The risk-based framework of protection was developed by looking at the threats and threats of smart objects that drive the IoT. The "Public key infrastructure" (PKI) is used to verify "IoT" networks. IoT-based, intelligent development processes comprise self-optimizing and coordinating the availability of resources and utilization development systems [17].

13.	Internet Of Things (IoT), Security Issues And Its Solutions.	Fahad Azam & Rashid Munir & Mehboob Ahmed & M. Ayub & Ahthasham Sajid & Zaheer Abbasi, 2019	Use of certain "Artificial Intelligence (AI)" to identify fake user's which can be applied to "Cryptographic techniques" to protect the network, which prevent it from any harm. Issues can be resolved by using encryption techniques on "IOT" devices [18].

3. Three-layer IoT Architecture

Within IoT, every layer is specified within terms of its functionality and the gadgets included in that layer. In the past year's multiple IoT systems have also been introduced, but there was no consistent consensus. Moreover, according to many researchers, the IoT works primarily on three levels, or three layers called [6]. Sensor layer, [7] Routing layer, and implementation layer, respectively. Growing IoT tier has related security problems inherent in it, Illustration 2. Displays IoT's simple design structure of three levels with respect to the sensors and innovations surroundings each level. All three layers are defined in brief below:

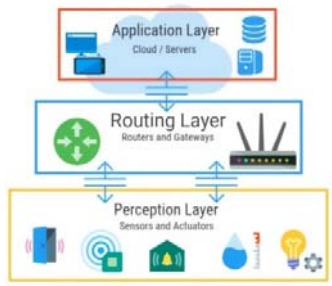

Fig 1 IoT Three-layered architecture [8]

3.1 Perception Layer

It is also known as a perception layer as it perceives information from surroundings by using actuators and sensors. This layer actually deals with data management; it identifies and collects the data by each category of the sensor unit. [9].The main purpose of this layer is to provide services to the network and to authenticate the devices[7]. Its framework often co-operates with the Internet of things nodes in regional and narrow-range channels. There are several forms of sensors connected to the hardware of items such as "RFID," "GPS Arduino," "magnetic strip," and QR Code. "Such sensors have been selected according to application requirements. The details such detectors gather might be regarding place, air change, climate, activity, vibration and etc. [1]. Devices in this layer have specific tags that enable good network communication with the majority of devices utilizing "Universally Unique identifiers." Knowledge transmitted from this layer is passed to the central processing layer or routing layer [7].

3.2 Routing Layer

IoT's network layer provides the feature of information processing via delivery across the internet between various IoT hubs and computers [2]. It's also called the transmission layer. This serves as a link between the sensor layer and the implementation layer. Its transmitting method could be wireless or cable dependent. It also shares the burden of linking smart stuff, network apps, and systems. Hence, threats from adversaries' perspectives are extremely sensitive [1]. This level is accountable for information security, machine communication, and knowledge maintenance via various protocols, such as MQTT 3.1 and CoAP Inside the connectivity in an IoT framework [7]. Cloud networking systems, Network gateways, filtering, and routing tools run on this network with some of the newest technology, including (Ethernet, LTE, Bluetooth, 3 G, Zigbee)etc. The system routers act as intermediaries among various Internet of things points by combining, sorting, and transmit data to and from multiple sensors [9]. However, information conveys reliably across the network layer to other layers [10].

3.3 Implementation Layer

Implementation of the application layer delivers resources according to customer request. For each application, its services can be different since utilities rely on the data that sensors gather [1, 6]. The information processed from the lower layers is used to produce useful end-user services. The information provides a platform for such applications that could benefit the user in many ways, including personal use of health education, gadgets, households, transportation, communication, etc. In IoT, security information should be equipped with features such as confidentiality, identification, etc. As IoT is being applied in various important fields such as health, transportation, industries, smart homes, postal services, and so on, IoT's security and privacy should be foolproof. The targeted approach should be defined for any protection factor [10].

4. IoT Layered Architecture with Security Attacks

Despite IoT's strong rate of growth, the increase of web-connected devices is rising day after day. Many

protection problems facing IoT levels, which are addressed as follows. :

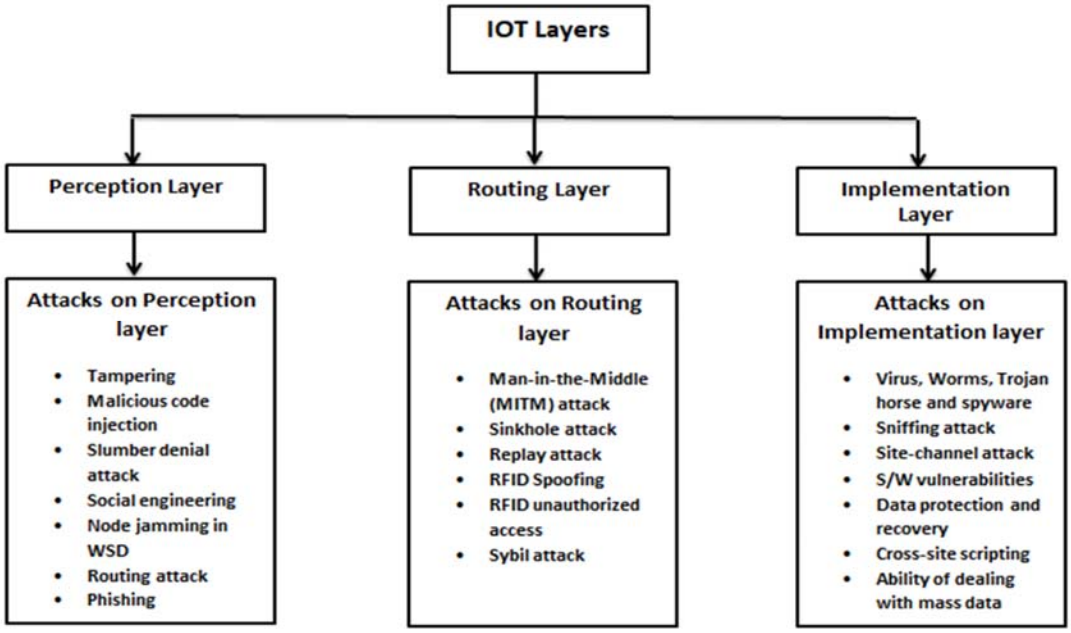

Fig 2 Attacks on the IoT layers

4.1 Perception Layer

Attacks on the sensor/perception layer appear to impact the mechanical parts of IoT that are fairly costly to execute due to the pricey complexity of the equipment and resources used to conduct it, so the intruder has to have direct interaction with the IoT network [7]. Different IoT gadgets such as smart wearables, videogames collect information about each other, and some cybercriminals may share or connect directly with this info for unlawful intentions [8]. Common security threats/attacks of the sensor layer are

4.1.1 Tampering

Tampering is an activity when an intruder makes external modifications on the computer or the connection channel. This external layer offers an excellent barrier to an attack. Device components could be hacked, identities compromised and modified, which may violate the rights priorities of security, functionality, or credibility. One way to eliminate this is by utilizing "tamper-resistant packaging" [11]. By modifying the computer interface or catching the gateway node, the intruder may access all of the details on the system, including route table, communications key, encryption key, wireless key, etc., and threaten the whole network, even higher levels [10].

4.1.2 Malicious Code Injection

Also known as Man-in-the-Middle Attack, by introducing a new malicious node between the sender and the receiver node, it appears to take on the communications channel. That intruder thus takes liability for data sharing between multiple points in the IoT network [7].

4.1.3 Slumber Denial Attack

Throughout the IoT network, devices in remote areas are mostly operated via removable batteries, and such devices are designed for sleep when they are not throughout operation due to battery savings. Intruder keeps the nodes alert to prevent them from snoozing by supplying fake feedback into the node resulting in a power failure, hence power failure of the node [2].

4.1.4 Routing Attack

Secondary deceptive endpoints may alter its straight configuration routes during data gathering as well as the routing process [12].

4.1.5 Social Engineering

The intruder connects and tries to manipulate IoT system clients physically. The intruder gets confidential details that reach the goals [13].

4.1.6 Replay Attack

It is regarded as the back-attack action. It is an intrusion where an attacker keeps tabs among the sender and recipient about the protection and removes truthful details from either the sender. An attacker delivers that same validated details to the person still obtained through showing evidence of the identification and credibility in the correspondence. The letter was encrypted so that the recipient may interpret it as a valid order and taking action against the attacker's needs [1, 8].

4.1.7 Node Jamming in WSNs:

The intruder will perturb the remote contact while using the transmitter. This triggers service assault denial [13].

4.1.8 Phishing:

Phishing scams relate to those assaults were a minor power placed by oppressors targets multiple computers. It's a form of stealing for identities. The risk of phishing emails is for users who visit webpages. Whether the intruder steals the customer's login and credentials, as well as the user whole IoT environment, becomes vulnerable, thus prone to internet-attack [8].

4.1.9 Access Fabrication

Intruders may use racial conditions to manufacture network access and enter a computer or network [14].

4.2 Routing Layer

The routing layer usually includes the sharing of data from the sensing/perception layer across the channel. Thread is increased for this layer as this layer gathers data from different heterogeneous machines. The key security issue is authentication and reliability of the content being transmitted inside the network layer. "IoT" system layer struggles from all sorts of security risks found within the context of computer networks. Attacks can build a complicated situation for the IoT community. Some network layer security issues are

4.2.1 Man-in-the-Middle (MITM) Attack

Attacker intrudes node privacy, accesses sensitive data, and often takes control of connectivity by controlling and interfering with IoT device sensor nodes. This attack does not require that the intruder appear personally at the network site. It can be achieved by the use of the IoT routing protocol. This attack may be eavesdropping, routing, and replaying attacks [15].

4.2.2 Replay Attack

It is an attack in which an attacker collects information from the sender and receiver and collects authentic info from the sender. An attacker sense similar authenticated info to the victim. You can overcome replay attacks by using "Message Sequence Numbers" and "Message Authentication Code" (MAC) [11].

4.2.3 Radio Frequency Identification Spoofing

The "Radio Frequency Identification" signal is intended for the "Radio Frequency Identification" spoofing intruder to gain access to the information marked on the RFID tag. Using the original Id, when the signal spoofed intruder uses, this too sends information. Now intruder got full machine control [10].

4.2.4 Sinkhole Attack

The intruder builds a promising sinkhole from various IoT WSN nodes for the data. The attack targets the security and privacy of info by preventing packets from being transmitted to their proper endpoint [7].

4.2.5 RFID unauthorized access

Tags are open to everyone because RFID systems don't have a secure encryption method. So tags can be easily affected [16]. The intruder takes advantage of the weak encryption protocol in RFID systems for tag access to alter, read, and delete sensitive data on the IoT system.

4.2.6 Sybil Attack

A neighboring node in wireless IoT network allows fake messages in this attack. The threat appears to contend that several nodes are known. In addition, Sybil targets the exploitation of equal use of IoT resources by the tool. Although obviously malicious nodes are fake, they actually operate as actual and true nodes, creating extra and unnecessary traffic on the computer network [17] [18].

4.3 Implementation Layer

Due to confidentiality problems, both the program could be exploited and disabled easily. The malicious assault will trigger viruses to breakdown throughout the computer program script that unlocks the device. Applications may often be abortive by bringing while validated services in which they are intended to erroneously operate or offer services [16]. Distinct

applications include various encryption methods, which make it difficult to incorporate them to guarantee data protection and verification of identity. Some major attacks which are associated with that layer given below:

4.3.1 Virus, Worms, Trojan horse and spyware

The program could be compromised by adversaries through vicious applications that can lead to knowledge licking, data manipulation, or unauthorized access [10] [19].

4.3.2 Software defenselessness

The device bugs may be enhanced by anti-standard code generated by programmers. The nasty people are using this tool to accomplish their unethical desires [16].

4.3.3 Cross-Site Scripting

This is an invasion via injection. This helps an intruder to inject a browser-side file, like java file, into a trustworthy web where many clients visited. By doing so, an intruder will totally alter the contents of the document according to his or her requirements and illegally use original information.

4.3.4 The ability to deal with Mass Data

Due to a massive huge number of computers, as well as a massive amount of data transmission between clients, it does not have the capacity to manage to process as required. As a consequence, it triggers disruption of the system and a lack of results [1].

4.3.5 Software Vulnerabilities

Security flaws exist as it was designed by developers leading to the non-standard code, resulted in buffer leakage. The attackers are using this tool or approach to attain their objective.

4.3.6 Data Protection and Recovery

Data transmission data requires consumer protection. Information could be destroyed, and incomplete architectures and information management and privacy protection systems may also result in severe damage. The maintenance of the mass nodes is one factor, too [10].

4.3.7 Side-channel Attacks

The intruder utilizes the information from side channels, which is released through encoding tools. It's neither a plain text nor text of encryption; it comprises energy information, the time required for the process, the frequency of flaws, etc. Intruder utilizes the data to detect the key to encode [13].

4.3.8 Denial-of-service attack

In this invasion, the intruder professes to be an authorized person and logs in to the program, interrupting the channel's normal operation. That is the Machine's greatest weakness [20].

4.3.9 Sniffing attack

In this case, the intruder adds a sniffer program into the device to impose an assault on it, which could obtain packet sniffers contributing to the compromised framework and combine program and web application layer to create the interconnected security mechanism.

4.3.10 Access Control Attacks

An attack on application control, where an opponent or software developers gain entry to the entire IoT arrangement. The primary reason for such an attack would be to take clear sensitive information as well as details, rather than destroy a machine [8].

5. Steps taken to protect the IoT Layers

IoT demands security precautions for all three layers; on the sensor layer for data collection, onto the routing layer for transmission, and on the application layer to protect confidentiality, verification, and privacy.

5.1 Perception Layer Countermeasures

5.1.1 Authentication of Devices

Endpoint authentication is an authentication framework intended to ensure that only authenticated machines are able to connect to a defined network, location, or operation. Until accessing the network, protection of the systems will be maintained to hold the malicious systems apart from either the IoT system, meaning that compromised information can be stopped from joining the system. The machine should never be able to interact with the system without appropriate authentication that blocks false data flow inside the network.

5.1.2 Software defenselessness

Every system in the IoT network will be supported by a mechanism for error detection, which significantly reduces the possibility of data tampering. There will be various methods for detecting errors, which are used as symmetry bit, checksum, etc. Hashing algorithm must be used to render this more efficient [10].

5.1.3 Anonymity

Hiding confidential information, including data address and location, is an essential prerequisite for preserving high secrecy of data when it passes across the network. Zero Information and K-anonymity strategies are usually applied in order to do this in the IoT network, but the K-anonymity technique appears to be the perfect strategy for IoT systems related to its low power usage efficiency [7].

5.1.4 Encryption

Encrypting Internet of things data utilizing encoding algorithms such as RSA, Blowfish, and AES will secure IoT devices from attacks since this turns the data into encrypting text such that an intruder cannot decode the content.

5.1.5 Risk Assessment

Using the Innovative Risk mitigation methodology, higher user confidentiality, and security towards attacks in the IoT network can be accomplished because it offers means of detecting various forms of threats to the system. In certain situations, where a mistake is found using the complex risk management system, RFID performs an auto-kill instruction of RFID identifiers. This, in turn, reverses unauthorized data access.

5.1.6 IPsec Security Channel

IPsec certainly provides two forms of protection features, authentication, and data encryption. Encoding data that guarantees the integrity of data can be prevented through eavesdropping and code tampering. The source of the data may be marked as being actual or not by the recipient, who is the source over the IP [15].

5.1.7 Physical Secure Design

The attack from the perception layer could be resolved by the safe physical architecture of edge routers. The computer modules, such as the radiofrequency circuit and chip range, have to be of good quality. Effective antennas architecture for wireless technology may be able to connect over a long distance [16].

Table 2 Perception Layer Attacks Analysis

Attack Name	***Action***	***Harm***	***Countermeasure***	***Layer***	***Type***
Tampering	Damaging information or external modification	Tamper-resistant packaging	Physical secure design [16]	Perception layer	Physical
Malicious code injection	Inserting malicious code in the network	Integrity	Secure booting and hashing algorithm [22]	Perception layer	Software
Social Engineering	Disclosure of private data	Disclosure of data	Encryption/ maintaining high data privacy [24]	Perception layer	Physical
Node jamming in WSN	Prevent valid packet from being sent and acknowledge	Availability	IPsec security channel [24]	Perception layer	Physical
Slumber denial attack	Prevent node from felling asleep	Availability	Authentication [15]	Perception layer	Network

5.2 Routing Layer Countermeasures

5.2.1 Data Integrity

Data integrity can be established through the application of cryptographic hashing functions. It means data as it hits the receiving side is not changed. Mitigation issues are overcome by using a mechanism for error correction [28].

5.2.2 Data Confidentiality

Confidentiality can be protected by prohibiting the IoT network nodes from illegitimately accessing them. End to end encryption can be used for purposes of authentication. Protected data in this step is automatically transformed into uncrackable cipher code [16].

5.2.3 Routing Security

Practically all devices in sensor networks require a reliable routing. To maintain privacy in certain routing protocols,

various routing techniques are implemented in IoT systems on the sensor network as data is shared on specific nodes. For routing reasons, the source routing strategy in which distributed data is preserved in packets after review before being processed for processing [15].

5.2.4 Spoofing

The spoofing threat can be dealt with by a GPS location system. No ideal solution for this issue is yet given, [29] identified what is best for the GPS system techniques.

5.2.5 Sinkhole Attack

Threats from within the system can be protected by security-aware ad-hoc routing and to stops inside attacks. Threats from outside the system can be protected by cryptography and authentication so that the intruder cannot access the IoT system. Security monitoring was applied to the packets of a route request; by evaluating the obtained data, the intruder can be removed from the system [16].

Table 3 Routing Layer Attacks Analysis

Attack Name	*Action*	*Harm*	*Countermeasure*	*Layer*	*Type*
MITM	Violate data privacy	Confidentiality	Strong data encryption [24, 25]	Routing layer	Physical/ Network
Sinkhole	Data leakage	All security levels	Ad hoc routing and stops internal attacks [16]	Routing layer	Network
Sybil attack	Node is injected and claims that's original node	Availability	Trusted devices identify to avoid [26]	Routing layer	Network
Routing attack	Network destruction of changing routing data	Confidentiality, Availability, Authentication	Routing attack prevention [15]	Routing layer	Network
RFID spoofing	Target RFID to get info on a tag to access the device	All security goals	GPS system technique [29]	Routing layer	Side-channel

5.3 Implementation Layer Countermeasures

5.3.1 Access Control Lists (ACLs)

Implementing laws controlling access control to user requests would help to track the IoT platform while maintaining device security and data security. ACL may work by preventing or enabling inbound or outbound traffic and tracks requests from other IoT users [7].

5.3.2 Firewalls

The authentication password and cryptography method could be broken due to weak login, so firewalls that monitor incoming and outgoing internet traffic must be used.

5.3.3 Use of Anti-virus, anti-adware, and Antispyware

This software is vital to maintaining the IoT environment's stability, accuracy, secrecy, and consistency [19].

5.3.4 User validation

Integrity and confidentiality systems are essential to a system's protection and safety because any protection compromise may be triggered by stealing information and inappropriate exposure to the IoT world.

5.3.5 Intrusion Detection Method

This detection system offers security options by triggering an alert if there is danger violation or unknown behavior on a network. Such a data mining strategy may be done by different methods to identify the operation [7].

5.3.6 Data Security

To prevent illegal access to the data, it is important to enforce encryption and safe authentication mechanism. This strategy would also maintain high secrecy of the data and safety of the whole IoT environment.

Table 4 Implementation Layer Attacks Analysis

Attack Name	*Action*	*Harm*	*Countermeasure*	*Layer*	*Type*
Virus, worms and Trojan horse	Vicious info leads to stealing personal data	Confidentiality, Availability, Authentication, and Integrity	By avoiding illegal site [26]	Implementation layer	Software
Data protection and recovery	Lost and harm private user data	The enclosure of confidential data	High secrecy of data [20]	Implementation layer	Physical
Site-channel attack	Preventing site channel info	Confidentiality, Integrity	Prevention methods [22]	Implementation layer	Physical
Software vulnerability	Use software and codes	Confidentiality, Availability, Authentication, and Integrity	Updating software and firewall implementation [15]	Implementation layer	Software
Sniffing attack	Use a sniffer to corrupt system	Data captured	System update and Anti-malware, Antivirus and encryption [15]	Implementation layer	Software

6. Protocols in IoT

6.1 MQTT

"Message Queuing Telemetry Transport" is a TCP based protocol for the transfer of basic data flows from sensors to middleware and applications. Any origin such as a sensor may publish its data so any user may request a subscription to the data. The MQTT interface is intended for resource-constrained systems that have a minimum bandwidth. It works on top of TCP and has three components. This implements a model of publication/subscription, where the structure comprises three key parts: publishers, subscribers, and brokers [21]. Publish/subscribe protocols must satisfy IoT specifications than request/response because clients do not have to send notifications, the throughput of the network is diminishing, and the need to use computational power is declining. There is a broker (server) in MQT, T, which comprises topics. The client may be a publisher who sends details about a particular topic to the or/and a consumer who receives email updates if there is a new change on a subject that he is subscribed to. The MQTT interface is built to sparingly utilize bandwidth and battery power. For example, Facebook Messenger already uses it. MQTT supports lightweight, low-power, low-memory apps [22]. To guarantee security, MQTT brokers allow TLS / SSL username/password verification, i.e., the same protection protocols that guarantee privacy for HTTP connections on the Internet.

6.2 AMQP

"Advanced Message Queuing Protocol" designed for the financial industry it also runs on TCP, which uses architecture identical to MQTT, publishes/subscribe. In these standards, the key difference would be that the broker is partitioned into two major components: exchange and ques [22]**.** AMQP offers asynchronous messaging collaboration between publishing and subscribe. The key advantage is its store-and-forward function, which guarantees stability even after interruption of the network. AMQP provides communication between publishing and subscribing through async messaging. The key benefit is its store-and-forward function, which ensures consistency even after a network disruption. The part of the exchange is responsible for collecting and delivering publisher messages to queues fulfilling pre-determined functions. Subscribers link to certain queues, that are essentially the topics, and provide sensory information whenever necessary.

6.3 COAP

The "Constrained Application Protocol" is a synchronous application layer requesting / responding protocol. CoAP intends to allow for the use of RESTful connections by portable tools with low capacity, processing, and interaction functionality. . It is a protocol directed to the network that facilitates low costs, dynamic routing, and to improve the efficiency of the function by including a convenient HTTP interface. CoAP will become the generic protocol allowing user connectivity and supporting IoT apps [23]. To maintain the entire functionality, lightweight CoAP operates over UDP. CoAP supports publishing / subscribing design, this software offers multi-cast interactions, and the publisher delivers the notification so that multi-subscribers can capture the

notification and take measures. The purpose of designing a UDP implementation layer protocol is built to handle resources is to eliminate the TCP overhead and minimize bandwidth utilization. The "Datagram Transport Layer Security" DTLS protocol is introduced to protect CoAP operations. Although CoAP was formed for "Internet of Things" and "M2M" communications, it does not involve any security measures that are built into it. CoAP assessment: it operates on the basis of the "REST" design, supports the requesting/ responding method, such as "HTTP."

6.4 XMPP

The "Extensible Messaging and Presence Protocol" was developed to communicate and share messages. It was developed across a century ago by the "IETF," making it a well-proven protocol which has been commonly used across the Web. XMPP protocol can resolve the requirement for IoT, as it allows short texts and low bandwidth; these features allow the "XMPP" protocol a better selection for the Internet of Things connectivity and texting. "Extensible Messaging and Presence Protocol" embraces the publishing/subscribing, model, which is more suited for IoT than the request/response method of CoAP. Distributed architecture allows for high availability in XMPP. XMPP assessment: it is easy and can be utilized in programs and systems that are heterogeneous. It's a scalable and versatile protocol; it has identified several extensions built on this protocol. Diversely, it has several drawbacks points, as this protocol requires a high memory utilization and higher CPU utilization, no Quality of Service assurance, and is limited to basic data sort [24].

7. Performance Discussion

This paper addresses the assessment of the security risks and their countermeasures to the Internet of Things network. The paper also discusses the consequences of these IoT security attacks, and also describes different countermeasures by which it limits IoT disruption and risk protection. Table 2, 3 and 4 present aspects of our performance evaluation, in which extensive exploration has been conducted.

8. Conclusion and Future Directions

The emerging Internet of Things (IoT) concept is fast making its way into our society, helping to raise the quality of society by integrating different mobile devices, innovations and applications. Generally speaking, the IoT will require anything around us to be automated. Several types of attacks have been invented with the development of technology to violate the security of IoT devices. This paper defined the three basic layers architecture and functionality of them and then discussed the protection vulnerabilities that can be exploited in these layers. We have described the countermeasures that can be taken to protect the IoT layers from the security threats describing a quick comparative analysis of attacks by defining prevention techniques, types, and effects of attacks on IoT. As IoT is integral part of our lives, measures should be taken to guarantee the user's protection and privacy. Ultimately, it follows that utilizing IoT is a very crucial thing, so keeping it secure is the primary consideration, and we can do so by implementing the solution mentioned above. This paper's effort is to get an insight into the issue in question (on IoT) and allow us to propose a better solution to address these issues. This review will be of immense benefit to securities researchers; it will help recognize massive iot security concerns and offer a comprehensive view of the risks, consider raising legal problems, exploitation and disclosure of data and privacy concerns.

REFERENCES

[1] Burhan, M., et al., *IoT elements, layered architectures and security issues: a comprehensive survey*. Sensors, 2018. 18(9): p. 2796.

[2] Mahmoud, R., et al. *Internet of things (IoT) security: Current status, challenges and prospective measures. in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. 2015. IEEE.

[3] Kumar, S.A., T. Vealey, and H. Srivastava. *Security in internet of things: Challenges, solutions and future directions. in 2016 49th Hawaii International Conference on System Sciences (HICSS)*. 2016. IEEE.

[4] Abomhara, M., *Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks*. Journal of Cyber Security and Mobility, 2015. 4(1): p. 65-88.

[5] Prasad, N.R. *Threat model framework and methodology for personal networks (PNs). in 2007 2nd International Conference on Communication Systems Software and Middleware*. 2007. IEEE.

[6] Kumar, J.S. and D.R. Patel, *A survey on internet of things: Security and privacy issues*. International Journal of Computer Applications, 2014. 90(11).

[7] Singh, D., G. Tripathi, and A. Jara. *Secure layers based architecture for Internet of Things. in 2015 IEEE 2nd World Forum on Internet of Things* (WF-IoT). 2015. IEEE.

[8] Ravindran, R., J. Yomas, and E. Jubin Sebastian, *IoT: A review on security issues and measures*. International Journal of Engineering Science and Technology, 2015. 5(6): p. 348-351.

[9] Pérez, S., et al. *ARMOUR: Large-scale experiments for IoT security & trust. in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. 2016. IEEE.

[10] Al-Qaseemi, S.A., et al. *IoT architecture challenges and issues: Lack of standardization. in 2016 Future Technologies Conference (FTC)*. 2016. IEEE.

[11] Varga, P., et al. *Security threats and issues in automation IoT. in 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*. 2017. IEEE.

[12] Vashi, S., et al. *Internet of Things (IoT): A vision, architectural elements, and security issues. in 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. 2017. IEEE.

[13] Naik, S. and V. Maral. *Cyber security—IoT. in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. 2017. IEEE.

[14] Frustaci, M., et al., *Evaluating critical security issues of the IoT world: Present and future challenges*. IEEE Internet of things journal, 2017. 5(4): p. 2483-2495.

[15] Chinanu, U.E., O.E. Oche, and J.O. Okah-Edemoh, *Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures*. Scientific Review, 2018. 4(10): p. 80-89.

[16] Rao, T.A., *Security challenges facing IoT layers and its protective measures*. International Journal of Computer Applications, 2018. 975: p. 8887.

[17] Aydos, M., Y. Vural, and A. Tekerek, *Assessing risks and threats with layered approach to Internet of Things security*. Measurement and Control, 2019. 52(5-6): p. 338-353.

[18] Azam, F., et al., *Internet Of Things (Iot), Security Issues And Its Solutions*. Science Heritage Journal (GWS), 2019. 3(2): p. 18-21.

[19] Kraijak, S. and P. Tuwanut, *A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends*. 2015.

[20] Ahemd, M.M., M.A. Shah, and A. Wahid. *IoT security: A layered approach for attacks & defenses. in 2017 International Conference on Communication Technologies (ComTech)*. 2017. IEEE.

[21] Frustaci, M., P. Pace, and G. Aloi. *Securing the IoT world: issues and perspectives. in 2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2017. IEEE.

[22] Deogirikar, J. and A. Vidhate. *Security attacks in IoT: A survey. in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. 2017. IEEE.

[23] Jain, A. and T. Singh, *Security Challenges and Solutions of IoT Ecosystem, in Information and Communication Technology for Sustainable Development*. 2020, Springer. p. 259-270.

[24] Ahmed, A.W., et al., *A comprehensive analysis on the security threats and their countermeasures of IoT*. International Journal of Advanced Computer Science and Applications, 2017. 8(7): p. 489-501.

[25] Khan, M.A. and K. Salah, *IoT security: Review, blockchain solutions, and open challenges*. Future Generation Computer Systems, 2018. 82: p. 395-411.

[26] Gautam, S., et al. *Recent Advances and Countermeasures Against Various Attacks in IoT Environment. in 2019 2nd International Conference on Signal Processing and Communication (ICSPC)*. 2019. IEEE.

[27] Swamy, S.N., D. Jadhav, and N. Kulkarni. *Security threats in the application layer in IOT applications. in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. 2017. IEEE.

[28] Chen, C.-M., et al., *RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks*. IEEE Transactions on parallel and distributed systems, 2011. 23(4): p. 727-734.

[29] Daneshmand, S., et al., *A low-complexity GPS anti-spoofing method using a multi-antenna array*. a a, 2012. 2: p. 2.

[30] Salman, T. and R. Jain, *Networking protocols and standards for internet of things*. Internet of Things and Data Analytics Handbook, 2015. 2015: p. 215-238.

[31] Salman, T. and R. Jain, *A survey of protocols and standards for internet of things*. arXiv preprint arXiv:1903.11549, 2019.

[32] Tukade, T.M. and R. Banakar, *Data transfer protocols in IoT—An overview*. International Journal of Pure and Applied Mathematics, 2018. 118(16): p. 121-138.

[33] Yassein, M.B. and M.Q. Shatnawi. *Application layer protocols for the Internet of Things: A survey. in 2016 International Conference on Engineering & MIS (ICEMIS)*. 2016. IEEE.