International Journal of Computational Intelligence in Control

Securing the Future: Comprehensive Analysis, Threat Mitigation, and A Robust Model for the Internet of Things

Muhammad Bilal[1]*, Waqas Khan[1], Muhammad Faheem Khalil Paracha[1], Muhammad Junaid Iqbal[1], Javed Iqbal[1], Adnan Abbas[2], Muhammad Fahim[3]
mbilal9k@gmail.com
waqasdurrani1993@gmail.com
faheemparacha.uettazila@gmail.com
muhammadjunaid.uos@gmail.com
javedmarwat7@gmail.com
malikadnan110@gmail.com
Muhammad.fahim1@wipro.com
[1]Institute of Computing and Information Technology, Gomal University, D. I. Khan, KPK
[2]Qurtuba University of Science and Information Technology, D. I. Khan, KPK
[3]Department of Cloud and Infrastructure Service (CIS), Wipro Arabia, Saudi Arabia
[1]*Corresponding Author: mbilal9k@gmail.com

Date of Submission: 10th April 2022 Revised: 16th May 2022 Accepted: 2nd June 2022

ABSTRACT
The Internet of Things (IoT) grapples with escalating security and privacy challenges, as the proliferating number of interconnected devices amplifies risks in applications, device authentication, and code vulnerabilities. With an anticipated surge in IoT adoption reaching 50 million devices, the specter of security breaches and hacking incidents looms large, underscoring the critical need for robust protective measures. This study systematically addresses IoT architecture's security intricacies, offering nuanced solutions through a comprehensive comparative analysis. As IoT networks facilitate seamless communication among devices across layers Perception, Network, Middleware and Application this research identifies and strategically mitigates security concerns, contributing to the fortification of a secure and resilient IoT landscape.

Keywords: ***Security, Privacy, Threats, Attacks, Challenges, IoT***

1. INTRODUCTION

The Internet of Things (IoT) is characterized as a "Physical Object Network," facilitating three primary relations: 1. Human to Human, 2. Human to Machine or Things, and 3. Machine or Things to Machine or Things, with communication occurring over the internet. IoT

encompasses diverse applications, including smart devices in areas such as transportation, health and grids. The analysis of IoT faces challenges in estimating limitations, including accuracy, recall, precision, and detection rate. Many datasets depicting various attacks, such as DoS /DDoS, Botnet, Brute Force, Web Attack, Infiltration, and Port Scan, contributes to the potential failure of IoT systems. [1]

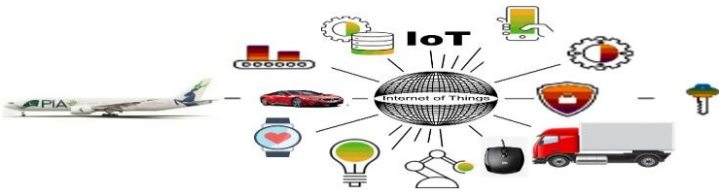

Figure 1- Internet of Things

1.1. Security Role in the IoT Development

There is increase in variety of the IoT applications and interconnected devices in IoT framework. On other hand, IoT technology is facing many security challenges. For example, many IoT devices like webcams, television and home alarms communicate over the network thus it could not offer the user to set up or enable the strong passwords for security reasons.

For the development of security mechanism, the security triad is the specific model. The data availability, confidentiality and integrity are the three major areas of implementation for the security mechanism as shown in the fig. 2.

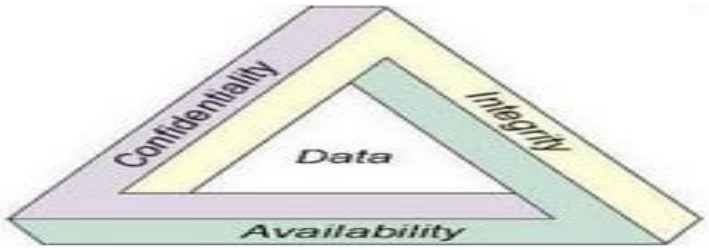

Figure 2- The CIA Triad [2]

Following are the Security Goals and their details:

Security Goals Table -1	
Data Confidentiality	Implement data encryption, converting information into cipher text to thwart unauthorized access. Employ a two-step verification process, requiring two identified components for secure sign-in, ensuring only authorized users gain access to the system.[3]
Data Integrity	During the transmission of the data integrity refers for protection of the sensitive data and useful information from the hackers. Data could be tempered without any knowledge
Data Availability	Immediate access to the authorized user should be granted not only in the normal condition but also in disaster condition. To countermeasure the attack, it is necessary to provide the firewall.

1.2. Security Challenges and Issues

In research field IoT has been got many achievements, but there are still many open challenges are needed to be addressed. In this section describe all types of security issues on every layer of the IoT architecture.

Security Challenges and Issues Table -2	
Perception Layer Challenges	Sensor technologies like RFID or other technologies were used in in perception layer. Threats on this layer described below.
Node Tempering	Hacker could replace the node. These nodes are the part of the hardware. Then in this way hacker could directly connect to it, alter the information and could get full access to the system. [4]
Fake Node	The hackers could make the fake node and could generate the malicious code through this fake node in the system. [5]
Side Channel Attack	Hackers exploit electromagnetic radiation emitted by sensor nodes to compromise the encryption mechanism. Attackers leverage power consumption and time consumption data from the sensor nodes for their malicious activities.
Physical damage	By using the Daniel of services (DoS) hackers physically damage the IoT devices because it this attack data would be unavailable to the user due to heavy traffic.
Malicious Code injection	Hackers compromise a malicious code and insert into nodes in this way he will get illegal access to the system. [6].
Protecting Sensor Data	In IoT system hackers can place the fake sensor and he could sense the same value by using this fake sensor, so confidentiality of data would be low.
Mass Node authentication	Network communication is required for authentication purpose only so nodes in IoT system face many authentication problems and it could affect the performance. [5].
Unauthorized Access to the Tags	Tags can be accessed by the hacker without any authorization because there would be the lack of the proper authentication mechanism. Hacker could read and delete the data in this type of attack.[7]
Tag Cloning	Hackers modified or change the tags by using different hacking techniques, so hacker could made replica of the tag and compromised so user could not differentiate between the original and generated tags.
Eavesdropping	It became very easy for the hackers to get the sensitive information for example password or any other type of the information due to wireless properties of the RFID. [3]
Spoofing	Hackers make or broad cast the fake information to the RFID system so that it looks real information and it show it generate from the real source. Hackers could get the full access to the system in this way.
RF Jamming	Hackers make RFID tags by using the DoS attack and hackers could communicate through RFID signal and interrupted with excess of the noise signal. [8].
Security Requirements of Perception Layer	IoT system should secure with all aspect. It should also be secured from physical access. To prevent from the illegal access node authentication is also more important.

1.3. Network Layer Challenges

This layer transmits the data from sensor to its required destination because this layer consists up of the wireless sensor network. The security issues related to this layer are described below.

Network Layer Challenges Table-3	
Denial of Service	Hacker generates fake traffic in the system more than its capacity and network would be unavailable to the user.
RFID Spoofing	In this type of attack, hackers could spoof RFID signal and then they could read RFID signal so, hackers send the fake data by using the original RFID tag and thus they could get the full access to the system. [9]
Routing Attacks	The hacker could disturb the network by altering the routing information. Hacker could also disturb the network by creating false routes, routing loops, dropping network signal and sending error messages. [10].
Sybil Attack	Hacker makes a malicious node and this node claim to identity the many nodes. It could distribute false routing information. [11]
Heterogeneity problem	Perception layer is made up of many heterogeneous technologies. A heterogeneity feature of the perception layer makes security and interoperability more challenging.
Network Congestion problems	Large amount of the sensor data used by the IoT devices. So, large numbers of devices are authentication at the same time so due to this network congestion occurred. [3].
RFIDs interference	Radio frequency signal used by RFID would be corrupted with noise signal in the network layer. So, it this way DoS attack would be occurred
Node jamming in WSN	Hackers interface the radio frequency of the wireless sensor network which cause deny of the services from wireless sensor network [12].
Eavesdropping Attack	In this attack hacker gathered information or sniff information by using some sniffing tools like packet sniffing because the wireless nature of the devices in network layer RFID or Bluetooth would be used to sniffing information. [13]
Sybil Attack	Hackers could generate fake node and manipulate this node to present multiple identities for this single node. This node would be considered as the part of the system and it could cause the false information about redundancy. [14].
Sinkhole Attack	Hackers could make node and it looks attractive to nearby node. All traffics which is going to through it would be consider that it has reached at their original destination.
Sleep Deprivation Attack	A sensor node in wireless sensor network uses batteries to keep the nodes awake. This attack consumed more battery power hence battery life time also is decreased. To extend the life time node are bound to sleep for a while. It caused shutdown of the nodes. [15]
Denial of Service (DoS) Attack	Network will be floated and not available for the user because the hacker made fake traffic in this type of the attack [16].
Malicious code injection	Hackers made a fake node in the system and generate the malicious code and inject it into the system. It is the serious kind of the attack in which complete shutdown of the system occurs [17].
Man-in-the-Middle Attack	The target of the hackers is the communication channel. Private communication between two parties could be control by unauthorized party. Fake identity of the victim without any knowledge would be generated by the third party. Thus, hackers could communicate normally to get the more sensitive information.
Network Layer Security Requirements	While the existing security parameters of the network layer are generally sufficient, notable security concerns persist, such as the distributed denial of services (DDoS) issue. To address challenges like routing attacks, congestion problems, and spoofing security, adopting robust communication protocols becomes imperative.

1.4. Support Layer Security

This layer is composed of data storage technologies like cloud computing. Security challenges of this layer are discussed below.

Support Layer Security Table – 4	
Data Security	Data could be secure with all aspect. It must be prevented or secured from breaches. Different tools should be used to detect the data migration from cloud, file, data base activity and data loss protection [17].
Interoperability and Portability	Among the cloud vender interoperability and portability is the major problem today. Who want to migrate from one cloud to the other cloud different venders uses different propriety standards creating problem for users. This heterogeneity creates security experience. [2]
Business continuity and Disaster Recovery	In the case of the natural disaster like fire, earth quick and flood, the cloud vender should provide the continuous services in such condition. In disaster condition, physical location should be suitable. Cloud also has some data backup plan. [2].
Cloud Audit	It is necessary to check compliance of these securities. For the cloud vender's security alliance set many standers.
Tenants Security	In tenants' data would be place at same physical device in the cloud and same physical device would be used to share the data is called tenants. Data of the user would be hacked by the hackers that are share at the same physical place.
Virtualization Security	Different venders may use different virtualization techniques. Network security could be bypass by using virtual machine communication. So, secure migration is required so it could hurdle in cloud audit. [2].
Unauthorized Access	Unauthorized access would be major attack for the system. This layer provided different interface for data storage facilities and for application. The hackers cause the real damage for the system by getting illegal access to the system so they can also delete the data.
DoS Attack	Hacker generates fake traffic in the system so in this way system became busy and data for the user would be not available at this time.
Malicious Insider	Hacker tampers the data for their own benefit or for 3rd party benefit. This could be done by hacker some sort of malicious code and data could be easily altered or extracted.
Support Layer Security Requirements	This layer provides data storage facilities for collected data. Between connected devices this layer acts as server. Standards should be continuously check and monitor. For the user online cloud audit mechanism is required it would build user trust.

1.5. Application Layer Challenges

Security issues related to this layer are described below.

Application Layer Challenges Table – 5	
Data Access and Authentication	In application layer there is a need of the proper access control and authentication mechanism because many users use many applications and different user has different access privileges.
Phishing Attacks	The hackers could get information by sending infected emails and web links. In this way hackers could get access to the system.
Malicious Active X Scripts	Hackers made an active x script and send it to user by using internet and user run this x script thus whole system would be hacked.

Malwares attack	Hacker steals sensitive data by using the malware. Different kinds of malware are used by the hackers like worm, viruses and Trojan viruses. It could cause the real damage and may exploit the system.
Malicious Code Injection	Hacker could inject a malicious code from user end and he would get access to the system and thus they could steal sensitive information
Denial-of-Service (DoS) Attack	Hackers generate fake traffic in the network due to heavy traffic data will not be available to the user.
Spear-Phishing Attack	Hackers send emails to the high priority person and force this person by own way to open this email when victim open it than hackers gain full access to the system and get all sensitive information while without the knowledge of the victim.
Sniffing Attack	Hackers made a sniffing application and attack into the system this cause damage or shutdown of the system and hacker also get the required information what they needed.
Security requirements of Application Layer	For application layer security purpose should use access control mechanism and strong authentication. Also encourage the user to use the strong password for better security. Best antivirus program should be used to control or protect from malware.

1.6. IoT Security Requirements

During manufacturing of the IoT devices proper security features should be adopted. During the manufacturing process or code making of the applications it should be ensuring that devices could not easily hacked and any malicious code could not be inserted by user. IoT security is based on three domains and would be discussing these three domains one by one trust, data confidentiality and privacy.

1.7. IoT Trust, Data Confidentiality, and Privacy

IoT Trust, Data Confidentiality, and Privacy Table – 6	
Trust in IoT	Trust and security are provided by the trust management infrastructure. Trust and security are based on credential and tokens these tokens are fixed also shared between devices. These tokens are used to identified in deflecting internal attack but failed to deflect internal attacks so, to control and handle the certificate public key infrastructure is used. It could also use Trusted Platform module (TPM) in the case of critical environment.
From a Device Perspective Trust and Security	The main problem related to trust management of these devices is a firmware. So, in this case internal attack may be occurred because attacker may insert a malicious code in the firmware and so they could access all sensitive information in the system. The devices with static firmware could maintain high level of truth worthiness, so it should dynamically update their firmware and upload mechanism has some sort of potential backdoor for the attacker.
Trust and Secure Key Storage	The key stores are used to increase the robustness of trust token. A key store is to act as storage for key, either as file or hardware device. The securities save and retrieve credential in the case of passive key stores.
Hardware Stores	It uses modern hardware security module. For managing crypto keys, special type of the tamper resistant devices is used.
Trusted Platform Modules	By trusting computing groups, trusted platform modules are made and these modules could be integrated with devices such as memories or also dedicated to microcontroller. The major function of this is to protect processing, booting, hardware and so on.
Software Stores	Software keys would be store in the devices and this is the natural key for storing keys and theses devices are physically connected to hardware module.
Identity Management	In layer of IoT based application, there would block of application integration so this limits the result. For manage and discover the IoT entities across the different solution there is no overall frame work exists to handle this.
Data Confidentiality in IoT	Node sends and receives data so it could be assured that data should be trusted. For example, wireless glucose reading to integrated insulin pump in a body area network. This information could be prevented in every aspect and data could be encrypted for patient security.

Privacy in IoT	Privacy means personal security information and also ability to control or check what happened to sensitive information in any serious attack. Privacy issues in IoT system would be complicated at every aspect.

1.8. Problem Statement

The Internet of Things (IoT) stands at the forefront of contemporary digital transformation, reshaping various facets of daily life, particularly in applications like digital healthcare. Embracing diverse hardware, communication protocols, and services, IoT brings both convenience and the challenge of numerous security threats. The crux lies in addressing security issues during data transmission, given that IoT devices, reliant on sensors for real-world data, are vulnerable to potential attacks by hackers. This research comprehensively explores security concerns and investigates emerging and existing technologies to establish a robust trust framework for IoT applications. The study advocates a thorough analysis of present and future security issues within the IoT framework to ensure consolidated protection. A detailed review of security challenges and threat sources in IoT applications forms a key focus of this research.

1.9. Research Questions

R1: How to identify the security issues at different layer of IoT generic architecture?

R2: How ensure the secure communication in any IoT devices?

R3: What are the tools to assess or control these security issues in IoT architecture?

1.10. Research Objectives

The research aims to accomplish the following objectives:

1. Identifying and analyzing the type of security threat at different layers of IoT generic architecture by different researchers in the literature.
2. Identifying the techniques or methods used in the literature to overcome different types of security threats at various layers of IoT architecture in order to ensure secure communication among different IoT devices.
3. Different tools are used to control the security issues in IoT architecture; aim is to identify which tool is more effective to handle what type of security threats.

2. MATERIALS AND METHODS

2.1. Proposed Structure

The comprehensive examination will delve into all types of security risks across every layer of the IoT architecture, encompassing aspects such as authentication, integrity, and confidentiality. Our primary focus is to meticulously study each layer of the IoT, elucidating all security vulnerabilities and attacks prevalent at each level. Given the interconnectedness of billions of devices within IoT networks, paramount importance is placed on prioritizing privacy. To fortify IoT security, a well-defined architecture will be presented, drawing upon the collective efforts of various researchers. Ensuring the stable evolution of secure technologies necessitates the establishment of a legal framework, coupled with sound regulations and policies. This research aims to categorize different attacks into distinct levels, comprising low-level, medium-level, high-level, and exceptionally high-level attacks, each delineated by their

severity. The overarching goal is to meticulously highlight all security issues inherent in the IoT architecture, providing not only a thorough discussion of each layer's security concerns but also offering viable suggestions for mitigating these challenges.

2.2. IoT, Privacy, Threats and Security Challenges

IoT change the life style of the human beings due to its autonomous facility and on other hand it still facing many security issues which are difficult to handle these security issues. In IoT every system need a proper security mechanism for betterment of the IoT devices. Security threats in IoT are described below.

Security Threats IoT Table – 7	
E2E Data	End to end data protection provide the in the complete network would be necessary to ensure the security of data in IoT environment. In IoT network devices could be connected each other and so data should be collected from these connected devices. So, there is the need of the proper frame work for protection of the data.
Secure thing planning	The interconnection and communication among devices may vary based on the situation. Consequently, it is imperative for the devices to possess the capability to uphold security levels under diverse conditions.
Visible/usable security and privacy	By the misconfiguration of the user many securities and privacy concern would be generated. Due to complex security mechanism and privacy policies, it would be difficult for the user to execute them.

2.3. Defining the IoT Threat Landscape and Solution Requirements

Simply without control over the security measure it would be danger to leaving the network endpoints without the proper security measure. For solution of the security risk in IoT four fundamental security risks security must be followed.

IoT Threat Landscape and Solution Requirements Table – 8	
Vulnerabilities	IoT devices are frequently designed or deployed without security considerations. Some may even be deemed "headless," lacking the capacity to execute security protocols or undergo updates.
Unsecure Communications	Devices utilizing public networks frequently communicate without encryption, transmitting data over unprotected networks. The traffic remains unmonitored, unmanaged, and unprotected.
Data Leaks	IoT devices serve as unmonitored and unmanaged entry and exit points to the network. Consequently, policies established to prevent data leaks may not effectively identify data passing through these devices.
Malware Infections	Unsecured devices have the potential to transfer or propagate malware. Once infiltrating the network, malware can spread from one device to another, posing a genuine threat and potential damage to the entire network.

2.3. Critical Elements of the IoT Security Solution

To control or manage the risk there would be need of professional expert for controlling these threats in IoT infrastructure. Proper strategies must be adopted to minimize the threats.

Critical Elements Table – 9	
Learning	Network parameter cannot be defined in the age of IoT. Visibility would be everything for the secure enterprises. When the new user power on the laptop then automatically proper security patches must be loaded for better security purpose.
Device Identification and Discovery	On the network there should be the need of the full view on every device on single dashboard. The snapshot that is completed may be change at any moment. There should be the proper mechanism that automatically detect any type of error occurred in the system on the network and develop comprehensive inventory devices.
Predictive Action	The upcoming challenge involves acquiring the ability to learn from performances and proactively respond to potential attacks before they occur. For instance, categorizing devices into Managed Devices (under your control), Allowed Devices (accepted but not controlled), and Rogue Devices (suspicious and non-compliant with policies) enables the system to learn the typical baseline activities for each category. This approach enhances the capacity to predict and counteract attacks preemptively.
Segmentation	Assigning policies and managing risk in the devices called segmentation. Segmentation protects the network in the case of the failure or protects the critical area from being compromised.
Identifying Risk	Classification could be first order in segmentation. To identify categories and assess risk user uses location, devices and data for this purpose.
Managing Policies and Devices	As the network expands, the discovery of new devices should be seamless, based on the configured devices. An effective solution is needed to monitor all device activities and establish appropriate policies.
Exerting Control	To safeguard the network, segmenting is imperative. By isolating IoT devices and other devices based on servers and ports, organizations can effectively separate resources according to risk levels, enhancing overall network security.
Protection	When IoT devices were part of the network and it is also secured it should protect with all aspect on the network.
Policy Flexibility and Enforcement	An adaptable solution should possess the capability to define and enforce policies on various levels, encompassing both device type and access. In addressing the intricacies of IoT, rules must be rigorously enforced to govern device behavior, specify the type of traffic a device can generate, determine its network location, and even ascertain whether it is permitted on the network at all.
Threat Intelligence	Which type of traffic in device would allow generating rules must be followed by governing the devices behavior to meet the challenges of the IoT devices? This all would be happened on the IoT network.

2.5. Identified Security and privacy Challenges

Now a day billions of people using internet but only some of them who properly know about the usage of the internet. Different heterogeneous devices were connected through internet capabilities in internet of things. These devices are increasing rapidly day by day and this led to less trust, security, adaptability and reliability. Security mechanism to IoT technologies cannot

be planned for its diverse communication standards and protocols. So, these devices may not be protected under these mechanisms. The most important challenges are as follows.

Challenges Table – 10	
Object Identification	Transmission between the objects could be monitor by the hackers and also gain the access to the system because the sensor network covers the huge area. Structure of object is insecure without data integrity[18]
Identity Management	Security challenges to identify the object uniquely complex relationship between interconnected things possesses it. A proper object identification method would be necessary. This is good to identify the fake object in the system.
Authentication and Authorization	Achieving authentication and authorization for objects involves utilizing various methods. For unique object identification, authentication, and authorization can be accomplished through ID passwords, cryptographic techniques, and database-driven access control systems. Authentication can be specifically achieved through cryptographic algorithms, ensuring a secure and reliable means of verifying object identities.
Privacy	The heterogeneity of interconnected devices has made it challenging to meet users' privacy requirements. Privacy is considered a fundamental human right, encompassing control over personal information and determining its permissible use. The discretion of sharing personal information rests with the stakeholders, allowing them the choice of either sharing specific details or opting for complete non-disclosure.
Input privacy	User input should remain confidential, safeguarded not only from unauthorized access but also from authorized receivers. It is imperative to protect user data from adversaries and potential attackers to ensure comprehensive privacy and security.
Output privacy	The authorized receivers should be the only one that deciphered computation output and it should only give access to its authorized user.
Function privacy	The foundational functions must be kept private and shielded from both potential attackers and unauthorized users.
Location Privacy	Location privacy is paramount, as its compromise could unveil comprehensive information about the user, including their personal living habits.
Network Security	Securing every layer introduces complexity. To meet these objectives, new privacy-enhancing technologies have emerged, including Virtual Private Network (VPN), IPsec, and Transport Layer Security (TLS). A TLS connection is essential to ensure confidentiality and integrity in data transmission
Identity Privacy	The distinction between the real user and claimed users underscores the importance of identity privacy, which must be meticulously safeguarded against potential attacks from the public domain. In emergency situations or disputes, the confidentiality of information can significantly impact the overall scenario, emphasizing the critical need for robust privacy measures.
Trust	Trust is a pivotal requirement in the context of IoT, given its distributed nature. Ensuring trust in IoT is paramount for its users, necessitating the assurance of trust in sensing devices, entity trust, and data trust.
Removing or Adding Layers	In a bid to maximize rewarded credits, social groups of IoT users may opt to remove connecting layers, effectively reducing the number of transmitters

	sharing the reward. This process, known as removing a layer, facilitates a more streamlined distribution of rewards within the social group.
Forward and Backward Security	Ensuring forward and backward security in IoT networks poses a challenge due to their heterogeneous nature. To address this, it is imperative to prioritize security and privacy for socially formulated user groups, necessitating the provision of both backward and forward security measures.
Lightweight Devices	Lightweight devices pose a challenge in IoT, as the small size of sensing objects and their lightweight processors can impede network performance. To address this, lightweight symmetric and asymmetric key management systems are essential to deliver reliable services and establish trust for users.
Object Compromise	Object compromise attacks occur when some adversary attacks the sensing device and extracts all the necessary and private information of the user as well as secret key.

3. PROPOSED MODEL

IoT sensors engage people and communities in collecting data but managing data security and privacy with traditional techniques would be a hard job. Upon intensive review, it has been found that there is lack of any such model which can provide finest security system for small sensing devices of IoT network. In this section, a model has been proposed (as shown in Fig) namely Security Enabled Model (SEM) to overcome security and privacy challenges in IoT systems. Proposed model detailed how small sensing devices could improve their applicability in real world scenario and eliminate the limitation of power consumption factor. To illustrate the performance of the proposed model, it is assumed when the sensing devices generate data from diverse places then that data has to be visualized by end users. Further, this model would be enhancing the power of small sensing devices in order to make comprised of four layers where each layer aims to provide security and privacy solutions and it also illustrates the sensing objects authentication and principles that IoT system should support Security and privacy mechanism, Quick responses and Data quality.

The proposed model was comprised of four layers where each layer aims to provide security and privacy solutions and it also illustrates the sensing objects authentication and principles that IoT system should support.

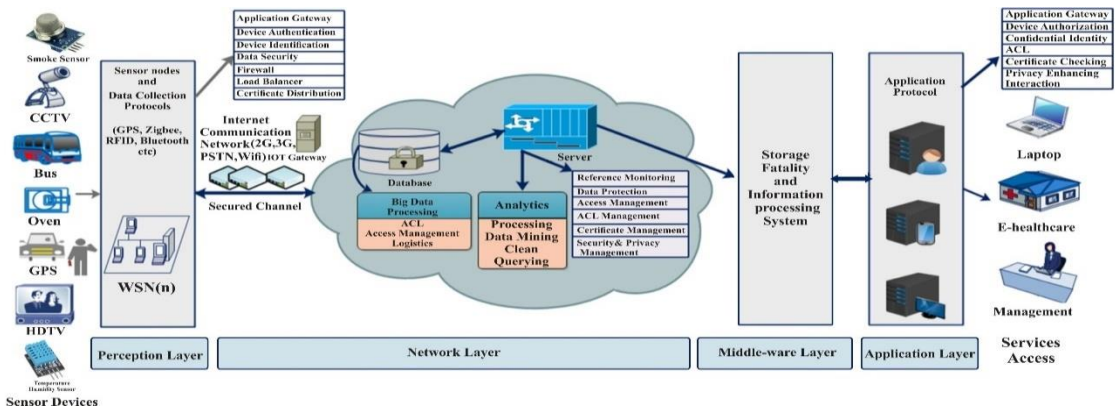

Figure 3 - Proposed Security Enabled Model (SEM) for IoT System

3.1. Python Code

```
class PerceptionLayer:
def display_user_interface(self):
# Code for presenting user interfaces
pass
class MiddlewareLayer:
def process_data(self, data):
# Code for processing data
pass
class NetworkLayer:
def communicate(self, data):
# Code for IoT communication
pass
class ApplicationLayer:
def run_application(self):
# Code for running IoT applications
pass
# Example Usage:
Perception = PerceptionLayer()
middleware = MiddlewareLayer()
network = NetworkLayer()
application = ApplicationLayer()
# Simulating the flow
user_input = Perception.display_user_interface()
processed_data = middleware.process_data(user_input)
communicated_data = network.communicate(processed_data)
application.run_application(communicated_data)
```

3.2. Network Layers

Network Layers Table – 11	
Perception Layer	The proposal advocates an authentication process for the inclusion of sensing devices into the network. This authentication involves an application gateway to scrutinize data from sending sensors, facilitating the identification of counterfeit objects by examining the contents of the sensing devices. Additionally, the implementation of a firewall ensures secure packet filtering, bolstering data protection from both internal and external networks. To fortify security, the inclusion of a load balancer and a certificate distribution system mandates that each device possess the requisite authorization certificate to become a part of the network.
Network Layer	A novel method of object identification is imperative, as the current IP technology is inadequate for IoT. In this model, the network layer transfers data to cloud servers for processing, establishing a secure channel to adhere to the proposed authentication process, wherein each object is identified, and their data contents are verified within the network. This layer encompasses collecting data from objects and routing it to the server for analysis, utilizing cloud gateways that offer data-driven application programming interfaces for efficient data collection. From the object to the server, cloud gateways are employed for storage and data analytics, incorporating Access Control List (ACL) management. The server acts as the central data processing center, providing secure analytic services, managing and evaluating reports, visualizing data, and handling queries. It is also responsible for maintaining and managing all data. To support user queries, new analytical techniques should be implemented, and the server, in turn, maintains the status of each object and checks the ACL for granting services to users. Servers employ data mining techniques for knowledge discovery and real-time analytics on data collected from diverse sources, be it structured, unstructured, or semi-structured. The model suggests a process for authentic database access, ensuring that only authorized administrators and users can retrieve the data.
Middle-ware Layer	This layer serves as the information processing system, facilitating the storage of collected data. Functioning as a bridge between connected devices, it handles database linkage and data processing. Notably, this layer is characterized by its application-independent software.
Application Layer	The model proposes data delivery techniques to minimize latency, enhance system throughput, and facilitate faster data retrieval. It incorporates Access Control Lists (ACL) to manage user access rights, allowing only those with certificates and the corresponding access list for interaction to access services. Various applications pose complex security issues, such as the risk of providing reports to unauthorized individuals. In the IoT environment, tackling the challenge of detecting fake objects is essential, necessitating the adoption of new technologies. Security challenges at the Application Layer involve authentication, data access restriction, handling extensive data volumes, ensuring data recovery, and identity authentication.

3.3. Requirements to Securing IoT Communications

In a network one device say a server to push the data to another device that would be IoT device and has to be listening. The listening devices will be open and inbound port in

traditional model and wait for the required data which will be pushed. This port must be remained open indefinitely so, it is the massive risk for IoT device. Code execution, DoS attack, theft of data, modification of data and malware infection are the major security risk leaving inbound port open. Devices should make only outbound connection to secure the IoT network.

3.3.1. End to End Encryption

For sending data over wireless area network transportation layer security is consider as industry standards communication layer to provide the true end to end security that would be paired with AES encryption. When the data transferred from device to device at end point transport layer security is suitable for transmission security. With advance encryption standard (AES) encryption specification data should be encrypted is necessary end to end security.

3.3.2. Token-Based Access Control

The primary challenge lies in achieving granular access control over the network, monitoring the senders and receivers of data. On the transmitting side, encryption by advanced methods such as AES and TLS enhances data security. With millions of devices attempting to access the correct channels and topics, the conventional approach of relying on end devices to filter out topics proves highly inefficient and insecure. Instead, the network should shoulder the bulk of this task. Introducing a token-based access control approach can efficiently grant access to specific data channels by distributing tokens to devices.

3.3.3. Device Status Monitoring

It is difficult to monitor online and offline status of the devices in the both consumer and industrial IoT. When devices like home security or home appliances disappear or stop sending and receiving data thus in this situation monitoring system should also know about that. Offline device could be tamper in this condition. Issues like power or internet outage has occurred.

3.3.4. User-Friendly Setup and Upgrades

In IoT devices work like user friendly environment. IoT devices operations would be assumed to connect with the internet. So, these devices work with automatically in the environment process of getting devices up, running, software and firmware update continuous basis for working them properly.

4. RESULTS AND DISCUSSION

The IoT vision aims to seamlessly connect humans and machines across diverse contexts. IoT devices seamlessly integrate into both wireless sensor networks and wired networks, enabling the creation of smart spaces, including smart homes, grids, transportation, traffic, cities, and health systems. However, the rapid expansion of IoT faces challenges such as ensuring availability, reliability, devising interconnection business models, and addressing security and privacy concerns. Through an in-depth literature review, this research focuses on identifying and addressing security and privacy challenges in the IoT environment. A robust security architecture is proposed, emphasizing security attacks and their countermeasures across the sensing, network, middleware, and application layers. The study explores existing and upcoming solutions, emphasizing the fundamental security requirements of confidentiality,

authentication, and integrity. Twelve categorized attacks, spanning low, medium, and high levels, are presented, followed by a comprehensive results summary offering insights and practical suggestions to effectively manage these security challenges.

4.1. A summary of different types of attacks and their threat levels, their nature and suggested solutions

Summary of Attacks, Threat, Nature and Suggested Solutions Table – 12			
Security issue	**Threat level**	**Behavior**	**Suggested Solution**
Node Tempering	Low level	Hackers can physically access to the sensor node so in this scenario hackers can replace the so in this way hackers can directly access to the system	We should apply the proper authorization mechanism. To perform specific task in the system only authorized person could access to the system and specific information.
Fake Node	Low to Medium	In this type of the attack hackers made a fake node in the system and generate the malicious code and inject it into the system. Complete shutdown of the system occurred and hackers get the full access to the system.	To detect the malicious user in the system, apply the authenticity to block this type of the user permanently.
Side Channel Attack	Low to Medium	Information like electromagnetic and radiation, time consumption and power consumption from the sensor node are used by the hackers to attack the encryption mechanism in IoT network.	Devices that perform communication we should apply proper encryption mechanism.
Physical damage	Medium to High	For DoS purpose hackers can physically damage the IoT device.	We should apply the proper data authentication to ensure that the information is not changed during the transmission.
Malicious Code injection	High	The hacker can insert the malicious code to the system and so he can physically compromise the fake node and hacker can get the full access to	Instead of the original data transmit the sample data and also apply anonymous data transmission.

		the system.	
Protecting Sensor Data	Low to Medium	For sensing the same value from IoT system hackers can place sensor near to the IoT system.	No route will be diverted to ensure the connectivity base approach.
Mass Node authentication	Medium	Authentication problem will be faced by the large numbers of node in IoT system. Authentication purpose only huge amount of network communication is required.	We should apply the proper authorization mechanism. To perform specific task in the system only authorized person could access to the system and specific information.
Unauthorized Access to the Tags	Medium to High	Due to absence of proper security mechanism in RIFID system without authorization tags could be accessed	We should apply the proper data authentication to ensure that the information is not changed during the transmission.
Tag Cloning	Medium to High	Tags data could be easily read because tags are dependent on different objects. Hackers can modify and read these tags by using different hacking techniques.	To ensure the security of the network and not information is changed during the transmission applies proper encryption techniques and authenticity mechanism.
Eavesdropping	Medium to High	To steal or sniff the sensitive information like password or other information from tag to reader became very easy for the hackers due to wireless characteristics of the RFID system.	Device that performs the communication should apply proper encryption mechanism.
Spoofing	High	Hackers in RFID system broad cast the fake information and this information would be assume that this information is generated from the original source	For cloning attack physically unlovable function is countermeasure. Apply identity base identification protocol to avoid from spoofing and cloning attacks.
RF Jamming	High	With the kind of the	To protect the network from

		DoS attack RFID tags can also be compromised and so in this condition n there is the excess of noise signal the communication through RFID signals will be disturbed.	such kind of attack we should turn on the fire wall, apply active jamming, anti-jamming, apply packet filtering and update antivirus program.
Denial of service	Extremely High	The hacker generate the fake traffic in the network so over burden of the traffic occurred so in this case data for the user would not be available	In order to protect the network from such kind of attack we should turn on the fire wall, apply active jamming, anti-jamming, apply packet filtering and update antivirus program.
Routing Attacks	Medium to High	In IoT network routing information could be alter by the hackers and this way he can create the routing loops by using the false routes by dropping the traffic or sending the error message.	No route will be diverted to ensure the connectivity base approach.
Sybil Attack	Medium To High	In Sybil attack identity of the many nodes could be claim the by a single malicious node	We should apply the proper authorization mechanism. To perform specific task in the system only authorized person could access to the system and specific information
Heterogeneity problem	Low	Perception layer is made up of many heterogeneous technologies. So, the access network has many accesses method. So, this heterogeneity features of the perception layer makes security and interoperability more challenging.	Hackers do not allow to fetch the information by using symmetric techniques ensure the confidentiality of data.
Network Congestion problems	Medium	In this attack devices are using large amount of the sensor data along with the communicating	This problem could be resolve by using the competent transport protocol and feasible device authentication

		overhead so this would cause the large amount of devise are authentication at the same time so due to this network congestion occurred	mechanism
RFIDs interference	Medium To High	By the RFID used radio frequency signals and these signals would be corrupted with the noise signals	To protect the network from such kind of attack we should turn on the fire wall, apply active jamming, anti-jamming, apply packet filtering and update antivirus program
Node jamming in WSN	Medium To High	Hacker interface the radio frequency of the wireless sensor network and this cause the deny of services from wireless sensor network	We should apply the proper authorization mechanism. To perform specific task in the system only authorized person could access to the system and specific information.
Sinkhole Attack	Low to Medium	In sinkhole attack hackers compromise a fake node and thus this node act as fake routing update in the system	Device that performs the communication should apply proper encryption mechanism.
Sleep Deprivation Attack	Medium To High	Node uses battery power in the network. So, in this type of attack node awake for the long time this consumes the more battery power battery life decrease and nodes will be shut down in this condition.	No route will be diverted to ensure the connectivity base approach.
Denial of Service (DoS) Attack	Extremely High	In Dos attack the hacker generate fake traffic in the system above its capacity and in this way, network would not be available to the user.	In order to protect the network from such kind of attack we should turn on the fire wall, apply active jamming, anti-jamming, apply packet filtering and update antivirus program.
Man-in-the-Middle Attack	Low to Medium	Hackers attack the communication channel. In this scenario all private communication between two parties can	To secure the data and information from stealing or modification before transmission proper encryption mechanism should be applied.

		be monitor and control by un authorized party.	
Data Security	Medium	To keep the data secure and confidential in the cloud it must be secure from breaches.	Different tools like data migration from cloud, file and database activity monitoring are used to detect data breaches.
Interoperability and Portability	Low To Medium	Among the cloud vender interoperability and portability is the major problem today. Who want to migrate from one cloud to other cloud different venders uses different propriety standards creating problem for user.	Venders should use same proprietary standards to overcome this problem for user
Cloud Audit	Low	To check the compliances of these security standards continuous audits would be required to build the user trust.	To build the user trust continuous audit would be required.
Tenants Security	Medium	User data may be located at the same physical drive in the cloud may share the same physical storage such are called the tenants.	We should apply the proper authorization mechanism. To perform specific task in the system only authorized person could access to the system and specific information
Virtualization Security	Medium to High	Security of the virtualization is very important. Different venders may use different virtualization techniques. To bypass the network security controls some time virtual machine communication is used.	secure migration is required so it could hurdle in cloud audit
Unauthorized Access	High	The hackers cause the real damage for the system by getting illegal access to the system so they can also delete the data	Device that performs the communication should apply proper encryption mechanism.

Malicious Insider	Medium To High	Hacker tamper the data for their own benefit or for 3d party benefit	Instead of the original data transmit the sample data and also apply anonymous data transmission.
Data Access and Authentication	Medium	Different user has different access privileges and other hand applications has different user.	We should apply the proper authorization mechanism. To perform specific task in the system only authorized person could access to the system and specific information.
Phishing Attacks	High	The hackers can get information by sending infected email and web links. In this way hackers can get access to the system	Hackers do not allow to fetch the information by using symmetric techniques ensure the confidentiality of data.
Malicious Active X Scripts	Medium To High	Hackers made an active x script and send it to user by using internet and the user run this x script thus whole system for compromise	We should apply the proper authorization mechanism. To perform specific task in the system only authorized person could access to the system and specific information.
Spear-Phishing Attack	High	Hackers send email to the high priority person and force this person by own way to open this email when victim open it than hackers gain full access to the system and get all sensitive information while without the knowledge of the victim.	Apply identity-based authentication protocol to avoid from spoofing and cloning attacks.
Sniffing Attack	Low to Medium	Hackers made a sniffing application and attack into the system this cause corruption or shutdown of the system and hacker also get the required information what the needed	Apply identity-based authentication protocol to avoid from spoofing and cloning attacks.

4.2. Summary

IoT architecture is studied briefly. Each and every layer in IoT architecture is studied one by one according to their functionality and all types of threats in every layer of IoT architecture is discusses one by one. These threats are categorized according their nature. These threats are discussed below.

Summary Table -13	
Low-level attack	When the hackers try to attack the network and attack did no successful.
Medium-level attack	When hackers just want to enter the network for just listening the medium and do not alter the information.
High-level attack	If an attack is carried on a network and it alters the integrity of data or modifies the data.
Extremely High-level attack	When hackers gain unauthorized access to the network and performing all illegal operations it could cause real damage in IoT devices.

4.3. How Much These Suggestions Are Effective?

. It is recommended not used the default password for better security purpose and read the security requirements for the devices before using it for the first time. Different security protocols should be studied that are used in IoT devices and network. By applying the above suggestion which is mention one by one in result and discussion portion the security issues in IoT devices would be handle in sufficient way.

5. CONCLUSION

In conclusion, this study addresses the escalating security challenges within the Internet of Things (IoT) landscape, prompted by the growing number of connected devices and the associated risks of applications, device authentication, and code vulnerabilities. With the imminent surge in IoT usage and the potential for unauthorized access leading to tangible damage, the imperative for robust security measures becomes evident. Through a comparative analysis, this research delves into the security issues across the four layers of IoT architecture Perception, Network, Middleware and Application proposing targeted solutions to mitigate these challenges. By offering comprehensive insights and practical recommendations, this study contributes to the establishment of a secure foundation for the future of IoT, ensuring the integrity and privacy of connected ecosystems.

REFERENCES

1. Nauman, A., Qadri, Y. A., Amjad, M., Zikria, Y. B., Afzal, M. K., & Kim, S. W. (2020). Multimedia Internet of Things: A comprehensive survey. *Ieee Access*, *8*, 8202-8250.

2. Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309
3. Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *sensors*, *18*(9), 2796.
4. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686-1721.
5. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646-1685.
6. Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, *77*, 103201.
7. Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International journal of computer applications*, *113*(1), 1-7.
8. Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of Things in agriculture, recent advances and future challenges. *Biosystems engineering*, *164*, 31-48.
9. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, *4*(5), 1125-1142.
10. Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *2015 IEEE symposium on computers and communication (ISCC)* (pp. 180-187). IEEE.
11. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *23*(3), 1622-1658.
12. Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, *22*(1), 196-248.
13. Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems*, *100*, 144-164.
14. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *Ieee Access*, *6*, 32979-33001.
15. Al-Hadhrami, Y., & Hussain, F. K. (2021). DDoS attacks in IoT networks: a comprehensive systematic literature review. *World Wide Web*, *24*(3), 971-1001.
16. Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on emerging topics in computing*, *5*(4), 586-602.
17. Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.
18. Falchuk, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. IEEE technology and society magazine, 37(2), 52-61.