e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

Mitigating the Security Issues and Challenges in the Internet of Things (IOT) Framework for Enhanced Security

Pankit Arora[1*], Sachin Bhardwaj[2]

Manager, Allowance & Loss Forecasting, National Money Mart Company, Canada[1]

Assistant Manager (IT Audits), MetLife GOSC, India[2]

ABSTRACT: Instead of depending on a technology's apparently positive qualities, we always have made it a priority to first examine its flaws. In addition to individuals and robots, now there are things that connect with the online platform without our input. These Things are continuously engaging with the Web, whether it's a refrigerator delivering an alarm about the foodstuff inside it or our vehicles sending signals to the technician about their fuel conditions. In many respects, the Internet of Things is brilliant. Unfortunately, the software has not yet been developed fully and is not totally safe. This paper summarizes the security risks and challenges associated with the internet of things, as well as offers suggestions for a few solutions for safeguarding the internet of things.

KEYWORDS: Internet of Things (IoT), Security, Attacks, Security framework, Security solution.

I. INTRODUCTION

Because of its broad possible applications, the Internet of Things (IoT) has received a great deal of attention. At the outset, many analysts expected that 2015 would be a critical year for IoT. Because of the recent rise of the internet, it has been predicted that the year could be the decade of the IoT Enterprise category. Questions were also voiced about slower development and advancement as a consequence of IoT security [1-4]. The public was persistent in highlighting the flaws and gaps in connecting any item to the web. The Internet of Things' security concerns are real, and they need to be addressed immediately. Nevertheless, it has also been repeatedly shown that each technological innovation encounters its fair share of challenges and critics. Although IoT security problems are inescapable, they should not prevent organizations from developing IoT applications. Figure 1 depicts a typical IoT infrastructure and its levels.

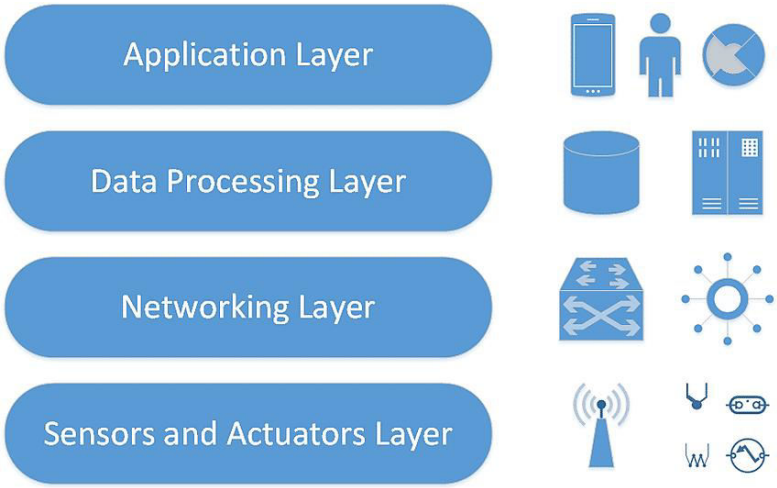

Figure 1. Characteristic IoT infrastructure Layers

As per credible IT businesses, the proportion of internet-connected gadgets may approach 50 billion by 2020. This enormous number of internet-connected gadgets represents a significantly bigger amount of data. Given the type of this

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

data, including people's personal data, bank information, health records, and so on, that is critical to investigate the flaws and obstacles in the privacy of such equipment and safeguard the data from possible exploitative activities.

But when relating to utilizing the Internet of Things, the most important worry of equipment that utilizes the internet of things is privacy. The computer in the internet of things could be private, commercial, or consumable; nonetheless, the information ought to be safe and protected from loss, modification, and transfer. As a result, in order to improve the security of the internet of things, special attention must be paid to the location of storage, the medium and technique of communication, the technique of cryptography, retrieval, and others.

1.1. Definitions and Standards

Nevertheless, there's no specific and generic description of the Internet of Things that is widely acknowledged, and academics and scholars have articulated their views with certain limitations based on their respective areas of study. Meanwhile, international bodies have provided definitions for the Internet of Things, one of the most generally recognized and utilized which is the one specified by the ITU in 2005. The Internet of Things is a worldwide information technology architecture capable of providing quality services using current or growing virtual or physical interconnections centered on things and appropriate data and communication technologies.

By extending and enhancing IoT technology, any gadget in the surroundings will be capable of communicating with some other types of equipment and providing data to them or operating them based on the data obtained. The Internet of Things encompasses technology solutions trying to connect to entities on the world wide web and maintaining connectivity between many decentralized entities, resulting in greater accessibility and establishment of new solutions including Wireless sensor networks (WSNs) that provide non-human-based solutions by linking multiple discs, and sensors of communication and information technology.

1.2. Security Challenges

The safety concern, particularly in terms of privacy and anonymity amid diverse organizational and increasing network limits, represents one of the fundamental difficulties confronting the implementation of the Internet of Things [5]. The safety and security of the Internet of Things must be reliable, economical, efficient, and functional in order to provide secrecy, authenticity, validation, and network management. For instance, consumers must be eager to disclose specific information regarding personal behaviors in online public places, and this need must be generated for the consumer only after taking the required precautions to avoid data leaks toward other individuals.

As a result, the system must safeguard the customer's security and privacy [6]. The fast rise of the Internet of Things in business and technology has opened up new avenues. Nevertheless, considering the dangers of smart home and vehicle connections, individuals are unwilling to compromise their privacy. As a result, increasing the amount of security and guaranteeing the protection of communications must be addressed that also necessitates improving the security of current communication systems or developing a new protocol set with a better safety standard.

Such difficulties in data management systems would then serve as the foundation for the legislation, that must be ascertained and affirmed concerning the legal structure for data security and the confidentiality of the Internet of Things since none of the conventional regulatory frameworks are appropriate for a distributed network such as the internet of things [7]. Due to the lack of consolidated rules or international norms in this field, it is critical to study and analyze current procedures in modernizing these and incorporating laws and standards between heterogeneous equipment.

II. LITERATURE REVIEW

Many academic publications have addressed the issues of privacy and security associated with IoT [8-16]. Many studies investigated safety and confidentiality, in addition to the available solutions that are offered. This study aims to explain the safety concerns present at each level of the Internet of Things by employing particular security methods. Nevertheless, there is no alternative option except to secure the perception layer.

Researchers exclusively discussed IoT safety in terms of essential safety concepts such as authenticity, reliability, and confidentially. When connecting through one computer to the other, the researchers advocated two-step validation utilizing biometric security, which does not apply. The recommended changes are not described in depth, and they additionally do not address the characteristics of IoT with comparable low-power components and massive network congestion.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

Limited research has looked into several smart house technology, such as sensing devices, smart home networks and devices, and smart home security platforms. The home automated prototypes were already presented to allow customers to wirelessly on/off any household equipment depending on the IoT infrastructure, as well as solar charger improvement. There are four kinds of experimental sensing utilized such as humidity sensor, intrusion prevention, infrared sensor, and carbon sensor module for controlling the Sensor module and automated environments. The testing field design, programming, and infrastructure have all been considered throughout the development's course of action. As a consequence, the house equipment has successfully integrated with the intelligent home's control scheme using switches. The results of the study in resolving security problems, risks, and needs offer sophisticated remedies for just one safety mechanism to manage access.

Additionally, several research studies have carried out a thorough investigation of the challenges of confidentiality and security in IoT networks. Nevertheless, they emphasized the fundamental challenges of IoT security as well as cybersecurity assaults. As a consequence of this investigation, different threat types are divided into four levels low, medium, high, and very high, along with associated proposed countermeasures.

Studies reported and examined key aspects of IoT security challenges. The report examined and identified the most common security problems associated with every IoT design layer, as well as the protocols used for administration, connectivity, and communications. Furthermore, the IoT security criteria have described the current threats and vulnerabilities. Furthermore, identifying the security challenges in IoT in comparison to remedies that exist in the literature was a component of the study. Lastly, they spoke about blockchain and how it could be utilized to tackle IoT security issues. Furthermore, investigators assisted the users in discovering the unoccupied space in the parking area, which would effectively cut the vehicle's time expenditure and fuel while looking for the space. The operation has been established to be done online via the internet.

The scholarly research was conducted in order to integrate Intelligent Transportation Systems (ITS) with the Internet of Things (IoT). The purpose of that kind of research study is to explore the potential of resource confidentiality, location identity, controller system, and grouping in ITS. Consumers may increase traffic efficiency by combining IoT and ITS. Investigators also have centered on two areas. The very first section defined and classified security problems in addition to remedies for ubiquitous computing.

Security concerns and solutions were classified on a variety of elements, including technical management and economic considerations. This categorization facilitates the monitoring of current safety measures, weaknesses, and dangers for various sectors of technology launched. The construction of smart cities was evaluated in the second step.

III. ARCHITECTURE OF IOT AND ITS SECURITY CONCERNS

Because of the wide range of IoT implementations, different IoT architectural types have emerged. It commences with a three-tiered framework (Figure 2).
The levels are as follows:

- Perception layer
- Network layer
- Application layer

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

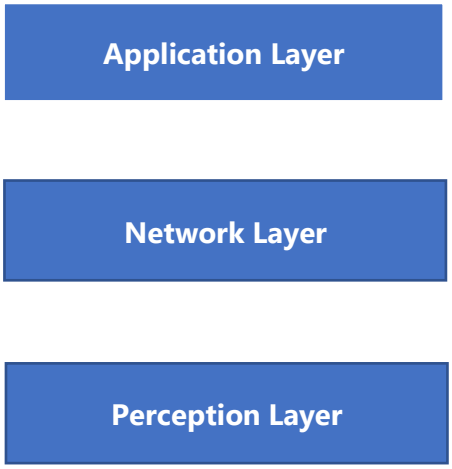

Figure 2. Three IoT layers

The perception layer, also known as the recognition layer, is just the bottom layer in the traditional IoT architecture. This layer has the responsibility of gathering and analyzing information from objects or the environments like Wireless Sensor Networks (WSN), heterogeneous networks, detectors, etc. Several alternative models incorporate a support layer between the application and the network layers. For instance, the ITU-T recommends a tiered IoT design with four levels. The upper part is the IOT application plane, which contains the application interface. The second level from the top is the service and application support layer. The network layer, which comprises connectivity and transit features, is the third layer. Lastly, the device layer, which includes the gateway, sensor, RFID tags, and so forth is the bottom part. The security capabilities, which are classified as generic and particular, are dispersed throughout all four tiers. Figure 3 depicts the layered structure of IoT.

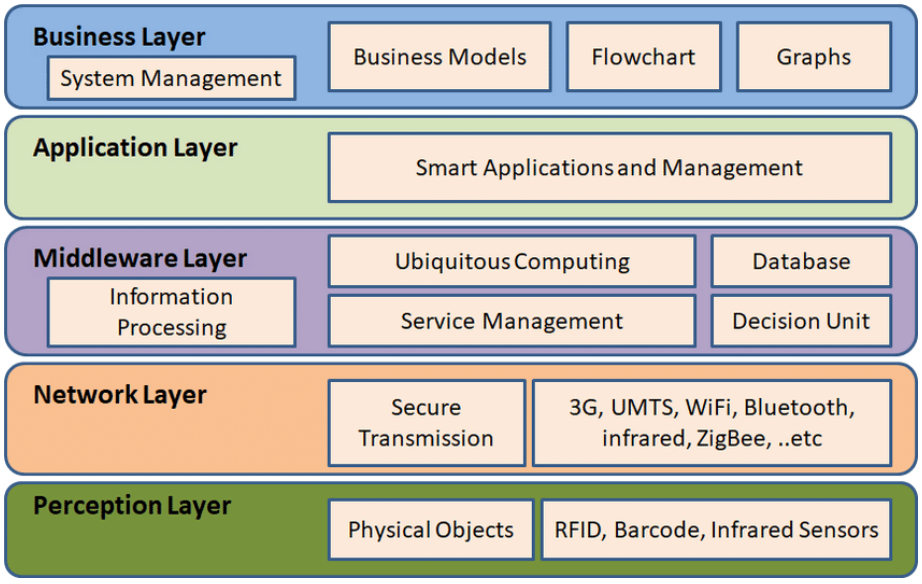

Figure 3. Layered IoT Framework

The IoT European Research Cluster (IERC) expands upon the IoT network by introducing the features that include in each layer. The networks and communication layer, for example, include network and communication functionalities like a gateway, forwarding and addressing, power minimization, QoS (Quality of Service), traffic shaping and trustworthiness, and detection and correction of errors. Authorization, key distribution and control, integrity, identity authentication, and verification are among the privacy management activities.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

Cisco has suggested a seven-level Internet of Things benchmark model to explain the capabilities. The Cisco IoT conceptual framework and its stages are depicted in Figure 4. In the framework, the flow of data is across both directions. In a monitoring structure, data travels from the highest level of the framework (Level 7) towards the bottom (Level 1), whereas control data moves in the opposite direction. The security protocols displayed in the Cisco IoT Reference must (1) protect every equipment or system; (2) protect all mechanisms at every stage; and (3) safeguard mobility and information exchange among each stage, regardless of whether north-bound or south-bound. As a result, as illustrated in Figure 4, security requirements are distributed throughout all stages.

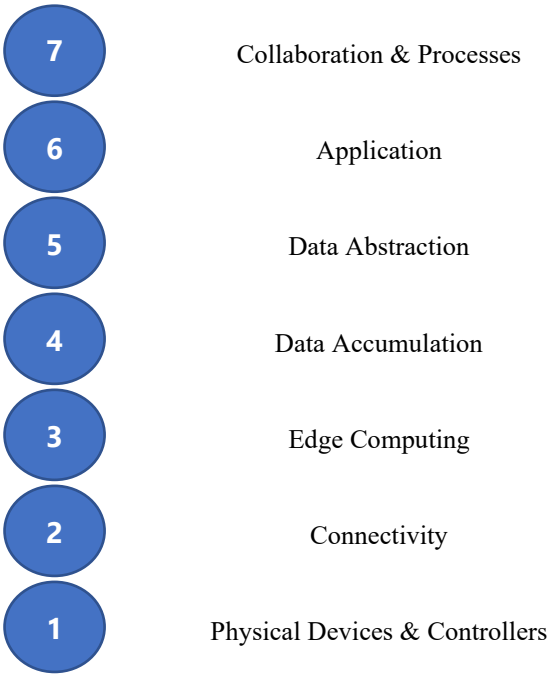

Figure 4. Stages of the Cisco IoT reference model

3.1. Threats and Complexities in IoT Security

There are 3 types of IoT threats such as threats that are common in any Internet network; risks that are unique to IoT systems; Security to make sure that no damage is inflicted by, assume, misappropriating sensors. The 2nd category includes specific issues related to IoT devices, such as the computers ensuring that all data is disrupted. A few IoT systems, for instance, are much too small to handle true asymmetric cryptography. Moreover, any gadget that could access the Internet has an existing software system installed in its system software, and a lot of these operating system processes are still not intended with a focus on security [17-20]. Numerous safety issues must be resolved so that reduced IoT services are accessible with a large number of gadgets interacting safely with one another. A few of the major issues are discussed below.

Scalability - is required when coordinating a large amount of IoT networks. Connectivity - a further task in IoT communications is securely trying to connect numerous gadgets with different functionality. End-to-end security precautions - are vitally valuable for IoT technology and Internet servers. Authentication and Trust - appropriate identity and authentication functionality, as well as their coordination inside a complicated IoT network, are still in their early stage. This prevents the development of connections among IoT components that are required for IoT applications that necessitate ad hoc interconnection among IoT components, like Smart City environments. To ensure that information analytics engines are served with reliable statistics, IoT trust management is necessary. It is impossible to guarantee that an entity's flow of data includes the information it is meant to contain without authorization.

Identity management - is an issue because poor security practices are frequently instated. It is prevalent, for instance, to use concise text/Base64 encoded IDs/passwords to equipment and machine-to-machine (M2M). This needs to be supplemented with organized tokens like JSON Web Tokens (JWT), which are utilized by the OAuth/OAuth2 authorization and security frameworks (the Open Authorization). Cryptographic Protocols that are resistant to attack -

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

because of the variety of IoT systems, security mechanisms that are both attack-resistant and easy to handle are required. IoT gadgets are susceptible to resource enervation attacks due to their restricted computation resources.

3.2. Risks and Threats on IoT Security

Interconnection between various threats was already proposed as an alternative name to emphasize potential risks in IoT. Undoubtedly, as shown in Table 1, IoT systems are especially susceptible to physical attacks, operating system attacks, side-channel attacks, and so forth.

Table 1. Threats in IoT Systems

Physical Attacks	Network Attacks	Software Attacks	Encryption Attacks
Node Tamper	Traffic Analysis Attack	Worms & Viruses	Side Channel Attack
RF Interfering	RFID Spoof		
Node Jamming	RFID Clone	Spywares	Cryptanalysis Attack
Injecting Malicious Node	RFID Illegal Accessing		
Physical Damages	Sinkhole Attacks	Trojan Horses	
Social Engineering	Man in the middle attacks		Man in the middle Attack
Sleep Deprivation Attacks	Routing Data Attacks	Denial of services	
Injection of Malicious codes in Nodes	Sybil Attacks		

Existing IoT systems are designed using technical solutions from a broad range of suppliers. A number of these systems are an interesting combination of elements retrieved from current systems for usage in particularly created frameworks, with the intention that the elements would function together securely. Security measures inside IoT elements, if present, haven't been built to compensate for the interdependence emerging from IoT connection characteristics. Industrial equipment, for instance, often lacks suitable security measures as they are supposed to be utilized in substantially secured and separated areas. Another illustration is the problem of delivering security updates or security fixes to final nodes in a reasonable timeframe while maintaining safety and reliability.

Extensive risk and vulnerability assessment methodologies, in addition to management systems for IoT systems, are necessary. Creating measures to mitigate IoT attacks necessitates knowledge of attack patterns as well as the series of events that occur when assaults occur.

3.2.1. Attack Classification Based on IoT Architecture

The IoT infrastructure is believed to have four levels in common. They will go through the primary security threats at the perception, network, and service levels in short. The four-layer system describes the most critical security challenges in IoT.

A. Threats to Cybersecurity at the Sensing/Perception Layer

IoT cybersecurity should be created and embedded into the gadgets directly in order to be completely implemented. That implies that IoT systems should be capable of authenticating their identification, retaining their validity, encrypting and securing their information in order to sustain integrity, restrict local database information and make sure confidentiality. The equipment security architecture should be stringent enough to protect data usage while still being dynamic enough to permit transitory secure interactions with individuals as well as other systems. For instance, although unlawful toll rate changes on a linked parking meter should be avoided, the meter must provide safe access for reserving and paying for a parking place for a specified duration.

Physical harm - Some hackers might lack technological competence, limiting such efforts to damaging electronics. Because equipment casings aren't always tamper-proof, computers may be unlocked and their equipment accessible utilizing probe and pin adapters. Tamper protection must be designed within equipment to make it impossible to remove critical data such as private information, encryption techniques, or passwords. Many gadgets are unable to safeguard their information and code against unauthorized users.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

As a consequence, an intruder may replicate complete systems or change their information and services, such as modifying a meter to generate erroneous values. A further case in point is the destruction of thousands of intelligent traffic light systems by criminals who seized the device' SIM cards. These seized cards have been then utilized to initiate mobile phone calls. Destruction of the roadway light system led to several automobile accidents and a large expense to repair the whole system.

The capture of nodes - Rather than eliminating the gadgets, a proactive hacker might obtain the data they hold. Sinkhole Assault - When devices in the system are left unattended for long periods, devices are vulnerable to sinkhole attacks. The infested node gathers data across all nearby nodes in this attempt. Forwarding Attack with Care - The attacker node may select messages and discard them, arbitrarily screening particular messages while permitting others. Lost messages could include critical information that must be processed subsequently.

Attack of the Witch - This incident comes whenever a hostile IoT node takes control of a genuine node's malfunction. When the genuine node goes down, the genuine connection routes all systems of the future via the compromised node, resulting in information destruction. Hello Flood Attacks - A hostile node starts a Hello flood attack by broadcasting Hello packets to all neighbors who are accessible there at the given frequency it has set. As a result, it is now a neighbor to all nodes in the network. The hostile node would then transmit a Hello packet to all of its neighbors, impacting network accessibility.

3.3. Security Concepts and Threat Classification

3.3.1. Internet of Things Security Practices

Below are the security concepts that are employed to share information in a safe manner among humans, applications, methods, and devices. In IoT, any transmission of messages between detector nodes must be safe. The information should be made available only to authenticated parties. The communications sent between networks must be incomprehensible to an attacker.

Integrity - It ensures that data is accurate. The recipient is prepared to detect if the communication has been altered by the adversary and to determine if the message originates from the legitimate sender. Authentication -The recipient should be able to identify the source of altered information. In contrast to message delivery, we would like to know whether a particular network, user or component is verified.

Authorization - IoT systems should be capable of determining the extent to which specific organizations are authorized to receive their recorded values. Only allowed entities should be capable of connecting to the IoT network at the network level. Unauthorised gadgets must not be allowed to route communications in the system, since this would waste resources. Freshness - ensures that no previous communications are rebroadcast. This may be critical in protecting transmission against replay assaults. Heterogeneity - An IoT platform should be flexible and robust since it links items or networks with appropriate characteristics, complexity, algorithms, and deployment versions. Policies - IoT networks utilize standards and guidelines to exchange useful data among devices. Because every component inside the network must be authorized and approved, present rules for both networks and computers do not appear to be appropriate, thus new policies and regulations must be developed.

Key Management Schemes - The transmission of messages concludes IoT device communication. Cryptography is required to maintain the confidentiality of data exchanged among devices in order to achieve network connection. To achieve encrypted connection, we need a framework of access control methods to impart confidence across completely distinct systems or entities and to transfer keys among the units.

Non-repudiation - A combination of assets and procedures is employed to demonstrate an entity's involvement in the data exchange. Availability of network services - Internet services must be accessible to both devices and nodes. Threats such as denial of service can seize control of the existing options, making the entity responsible for network measurement. The most fundamental concept is confidentiality. The harmful gadgets' access to individual data must be prevented.

3.3.2. IoT attack categorization

Security assaults are classified into five kinds. Physical attacks -These threats deal with the operating system of the computer and therefore are more challenging to carry out because they necessitate expensive materials. As an example, chip de-packaging, formant reconstruction, and numerous others. Side channel attacks - Because communication

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

happens between sender and receiver, a cryptography procedure is required to encode and decode information. This technique uses data from the encryption algorithm to retrieve the suspect and stolen device key.

Cryptanalysis attacks - are employed to disrupt data encryption and disclose details inside the Internet of things. Software assaults - Software attacks take advantage of implementation flaws inside the computer via its interfaces. Virus programs introduce malicious software into the system, causing it to malfunction. Network Assaults - These sorts of assaults specific network devices and appliances as well as channels of communication.

3.3.3. Layered Security Issues in IoT

Perception Layer

Sensor devices of various types are utilized at this level. RFID, ZigBee, and other sensing technologies remain widespread. When information is captured, the communication network is used to communicate with other devices or networks. Because a communication network is used, the foundation of communication is in signals that are broadcast in publicly. If proper precautions are also not implemented, the messages will be easily noticed, collected, and taken aback. Access to data in different sensors is manipulated by hackers. The following are common forms of attacks:

The capture of Nodes - Physical assaults is what they are. The network's nodes are hacked, disclosing information on the functionality of all nodes, thereby jeopardizing the safety of the whole network. The intruder installs a gadget into the system with a forged set of instructions or data, that might prevent the flow of authentic data throughout the system. The sleep of node energy is restricted, and the fraudulent node denies it. False nodes spend a large quantity of node energy and allow entry to or destroy the whole network.

Denial of Service Attack - This is the rationale for blocking network infrastructure and avoiding its use. It represents the most common kind of assault that typically occurs in Wireless Sensor Networks and the Internet. Timing Attack - By performing cryptographic techniques and examining the time required, important information may be retrieved. Threats to Routing - Because the system is wireless, packet forwarding is unpredictable. These assaults are much more common given that there is no defined route from the target to the source. Router nodes may be added or removed to lengthen or reduce the route, halt network communication, interfere with or repeat network data, generate new warning messages, and raise latency.

A playback attack - is another name for a replay attack. The receiver will receive a message delivered by the intruder in order to gain access to the platform's trust. The authorized and validated certification may be harmed by an assailant's communication. To connect with the upper levels in the perception layer, the IoT security architecture and sensor devices and capabilities are employed. It is additionally known as the sensing layer. The sensing layer collects data via various sensors. The IP techniques in use for network-to-network communication among devices are provided by the network level. The Application Layer is employed to assess technologies and programs for interoperability.

3.4. Attacks in Network Layer

Conventional Issues - Data connection among devices in the network will also have specific security vulnerabilities that may jeopardize the confidentiality of information. Despite the existence of appropriate security mechanisms in older systems, there continue to be certain common concerns such as unauthorized users to the whole communication network, data breaches, and security breaches.

Compatibility issues - Because the system is tailored to the individual's eyesight, as a result, there could be hardware compatibility when communicating data across different networks or computers within a single system. To split the coherence connection among IoT devices, current security techniques are applied. Different privacy causes scalability and networking synchronization to deteriorate.

Security Issues in Groups - Aside from internet blocking, there is the issue of verification, etc. The system is made up of several components. If it employs the present method to verify the devices, a huge quantity of packet forwarding would most likely cause the system to become unavailable. The existing IP architecture cannot cope with a large number of node identifications. Notice about Privacy Practices - And through the advancement of information retrieval as well as social networking, intruders may effortlessly acquire a large quantity of user data protection.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

3.5. Application Layer

Security concerns change depending on the industry or the environment. There are no standardizations in the architecture of IoT. Hardware connectivity is used in several sectors. It aids in the realm of healthcare sensing operations. The above layer often encounters the following issues:

Data Access Restrictions and Identity Verification - Numerous internet users utilize various programs. A single program could serve a significant number of users. An efficient security mechanism is required to prevent unauthorized user access to the program or networks. Malicious information or trash is readily discovered. Data Protection and Recovery - Communications among networks necessitate the confidentiality of the user. Techniques and procedures that have been designed and employed for information processing and security, but are unclear, cause the loss of information and are regrettable.

The Capability to Handle Mass Data -IoT is a WSN that comprises a big collection of linked nodes in which an abundant amount of information transfer occurs, resulting in a complex system architecture. Processing of data and scalability are insufficient to fulfil specifications, resulting in system disruption and the possibility of information leakage.

Application Layer Software Exposures - When developing software, trainers provide non-traditional commands that cause issues, and hackers may simply get access to the information and use it for their objectives.

IV. INTERNET OF THINGS APPLICATIONS

Some interesting Internet of Things (IOT) applications include (a) IoT-Enabled Health Care (b) Intelligent City (c) IoT-powered Connected Vehicles (d) Intelligent Home (e) Intelligent Agriculture (f) Smart Retail (g) Intelligent Supply Chain.

A. IoT-Enabled Health Care

In healthcare, IoT applications vary from distant monitoring devices to advanced and intelligent sensors to equipment integration. It possesses the ability to revolutionize the ways doctors provide treatment by also keeping their patients healthy and safe. Health IoT enables patients to spend additional time connecting with their physicians, increasing patient involvement and happiness. From fitness training sensors to robotic surgery, IoT in health introduces additional tools that seem to be up to date with the newest technologies in the environment, assisting in the improvement of health. IoT can help to create changes by providing cost-effective alternatives for both patients and doctors.

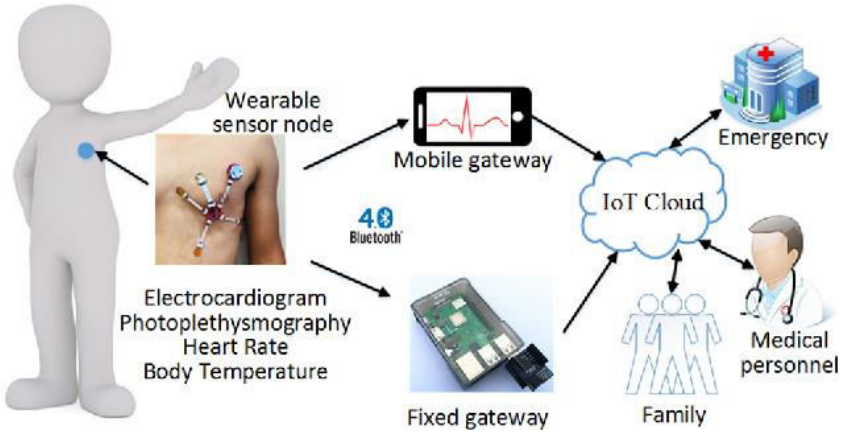

Figure 5. IoT-Enabled Health Care

Healthcare is still a huge piece of Internet of Things applications. The notion of a linked health system and intelligent medical equipment has immense promise not only for businesses but as well as for people's well-being in particular. According to studies, healthcare IoT would be significant in future periods. The goal of healthcare IoT is to enable individuals to live better lives by wearing interconnected gadgets. The information gathered would aid in the individualized study of an individual's well-being and the development of tailored approaches to treat sickness. Figure 5 depicts how IoT might improve health support and care.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

B. Intelligent City

A further significant IoT application that has caught the interest of the global public includes smart cities as shown in Figure 6. Internet of things technologies for smart cities include smarter surveillance, smarter systems for energy management, autonomous transportation, water distribution, urban safety, and environmental control. IoT will tackle key urban issues such as pollutants, road congestion, and power supply shortages, among others. Whenever a container has to be cleaned, technologies like the cellular-enabled Smart Belly garbage will notify local authorities. Residents may identify free parking spots throughout the neighborhood by placing sensors and utilizing mobile applications. The sensor may also identify meter manipulation, basic failures, and any setup difficulties in the power grid.

Figure 6. IoT-enabled smart city

C. IoT-powered Connected Vehicles

The emphasis of automobile digitalization has been on improving the vehicle's inner functioning. However, this focus is shifting to improving the in-car experiences. A linked automobile is an automobile that can improve its operations, servicing, and passenger safety by utilizing internal sensors and internet access. Most auto manufacturers, in addition to a few daring entrepreneurs, are developing connected automobile systems. Tesla, BMW, Apple, and Google are all aiming to usher in the forthcoming automotive transformation. Figure 7 shows the IoT-powered connected vehicles.

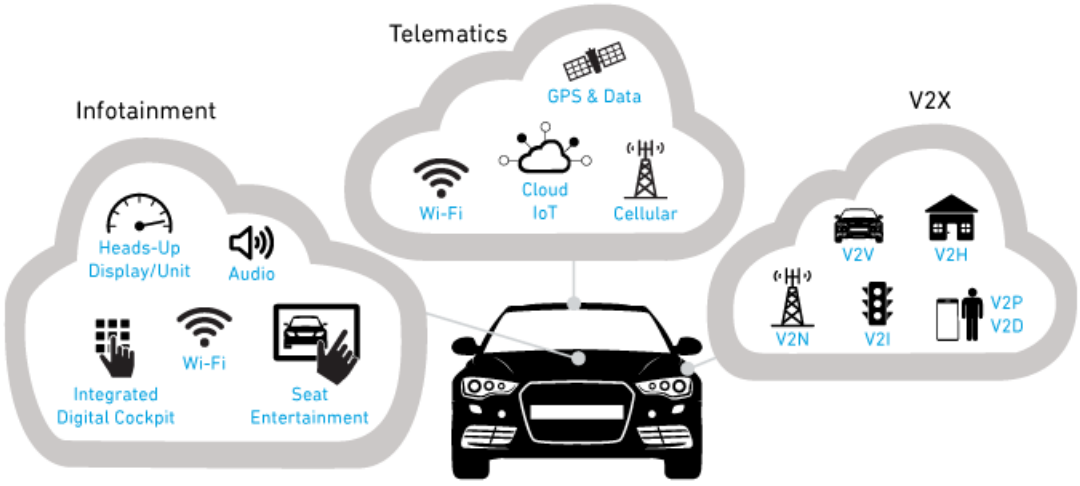

Figure 7. IoT-powered Connected Vehicles

The term connected automobile technology refers to a broad and comprehensive collection of various detectors, transmitters, integrated development environment, and innovations that aid in interaction in order to understand our complicated environment. It is in charge of rendering judgments with reliability, precision, and quickness. It should also be dependable. Such standards are going to become more crucial when people relinquish full control of the wheel and braking to the driverless or robotic cars that are already checked on our roadways.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

D. Intelligent Home

Intelligent homes, as seen in Figure 8, have emerged as the breakthrough level on the domestic achievement scale, and it has been projected that they will be as prevalent as cell phones. Whenever one conceives about IoT applications, the much more significant and effective application that comes to mind is Smart Home, which ranks as the top IOT application across all platforms. The anticipated level of funding for Smart Home businesses surpasses $2.5 billion and is constantly increasing. It would be great to be able to turn on the air conditioning when one arrives house or switch off the lights after leaving the home. Or give temporary access to your doors even while one is not at home. Manufacturers are creating products that will make everyday life easier and more comfortable as the Internet of Things takes form.

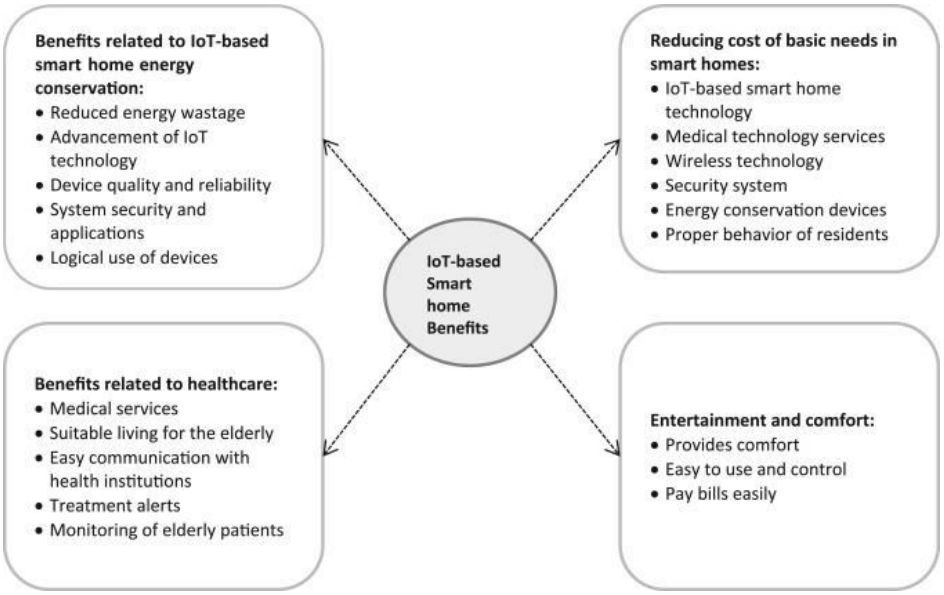

Figure 8. IoT-enabled smart home

The expense of purchasing a home is the single most expensive expenditure in an owner's life. Smart Home devices are advertised as time-saving, electricity, and budget. Intelligent home startups like Nest, Ecobee, Ring, and August, to mention a very few, can become household names and will offer a never-before-seen service.

E. Intelligent Agriculture

Smart agriculture is a frequently ignored Internet of Things application. Nevertheless, since most farming practices are detached and farmers deal with a big amount of cattle, the Internet of Things can manage everything involved and transform how farmers operate. However, this concept has failed to gain widespread traction. Nonetheless, it is among the IoT applications which should not be disregarded. Smart agriculture (Figure 9) does have the ability to develop into a significant application sector, particularly in agriculture trading nations.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

Figure 9. Intelligent Farming

F. Smart Retail

Businesses have begun to implement IoT solutions and use IoT intelligent systems in a wide range of applications that enhance retail operations including boosting sales, minimizing fraud, allowing inventory control, and improving the customer buying experience. Physical retailers can operate effectively with online competitors due to IoT. Companies may reclaim their diminished market share and draw customers further into the shop, allowing customers to purchase so much while cutting costs. Figure 10 depicts the expected use of IoT.

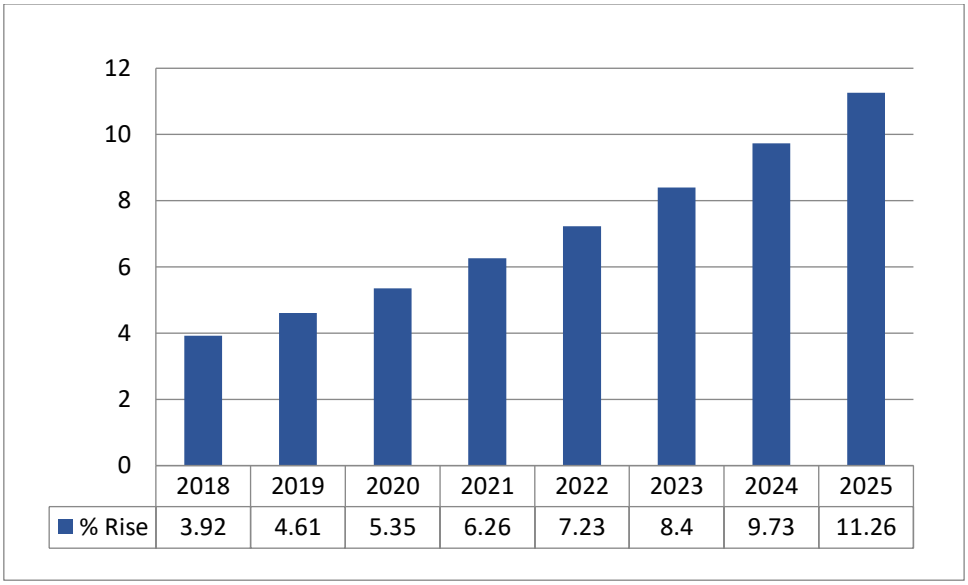

Figure 10. Expected use in the United States

IoT has huge promise in the retail industry. IoT allows merchants to engage with their consumers and improve in-store experiences. Cell phones will allow shops to stay in contact with their clients when they are not in the shop. Customer interaction using cell phones and leveraging online technologies may help shops better service their customers. They could also follow a customer's route through a shop, which allows them to enhance the shopping experience and locate expensive items in prominent locations.

G. Intelligent Supply Chain

For some decades, supply chains are becoming smarter. Among the most popular platforms include monitoring items while they are on route or on the journey and assisting vendors in exchanging inventory data. Industrial infrastructure

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

with integrated sensors communicates information about various characteristics including temperature, humidity, and equipment usage via an IoT-connected platform. To boost efficiency, the IoT platform may also execute processes and adjust equipment settings. Table 2 shows the impact on the smart supply chain by the IoT.

Table 2. IoT's Impact on Smart Supply Chain

Delivery Function	Impact of IoT	IoT Strategy
Warehousing	Time-saving till 99%	Smart things RFID tags
	Reduction in processing time	RFID Tags, Sensors
	Collaborative warehousing	Smart things & Multi-agent systems
	Warehouse management	Smart things
	Security and privacy	Smart things & Multi-agent systems
Order management	Data sharing	EPCglobal
Inventory management	VMI via real-time visibility	Smart things

V. RECOMMENDATIONS FOR IOT SECURITY SOLUTIONS

The only approach to reduce the device security vulnerabilities of the internet of things is to implement a comprehensive methodological approach. Certain security mechanisms as well as some important recommendations are addressed further below.

A. Device Variety

The distance covering networks of the IoT system is crucial. Once it concerns application or device's range measurements, one ought to be quite exact. For instance, whether one is utilizing a Zigbee module to operate the computer's networking, one has to find out the number of transmitters required within a building to provide adequate connection distance for the computers. Unfortunately, one might simply add an unlimited amount of transmitters since the computer's power decreases as the quantity of transmitters grows. As a consequence, network range analysis would enable one to identify the perfect spot whereby range may be optimised before crossing the restriction.

B. Latency and Capacity

The network's capacity is measured in bits per second (bps), whereas latency is the overall duration it takes for information to travel among application destinations. Designers are continually searching for methods to enhance capability and latency in existing IoT apps to boost efficiency. The issue is that the above two parameters are inversely proportionate, thus enhancing one decreases another. In data-intensive applications and systems latencies and resource balance must be monitored closely.

C. Manufacturability Test

It is uncommon for someone to design their personal IoT system from the bottom up. Throughout many circumstances, third-party elements and devices will be used in the software. It is critical to test such components to ensure appropriate functionality. Producers conduct their own production line testing, therefore it is possible to double-check. Furthermore, after all of the elements have been placed on a circuit, testing is required to guarantee that no fault has indeed been created through solder and cabling. Manufacturability testing is necessary to confirm that the product works properly.

D. Creating Strong Passwords Often

In recent times, altering credentials on online accounts, desktops, and portable devices on a regular basis is now the norm. By then so, it should have become routine for Internet of Things devices. Every IoT platform does have its unique password, which should be updated at minimum once a year to avoid utilizing common or general credentials and to create exceedingly hard and tough to break. Credential managers can assist in remembering it all since they may also be compromised.

E. Avoid stating cloud computing

Although cloud computing technology is simple, it is nonetheless a highly unsafe and attack-prone revolutionary innovation. Each device purchased with an IoT vendor often includes cloud storage capacity. Regardless of how attractive to pick something free, take into consideration that retrieving stored information in the cloud needs an active link, that could be accessed when a person using cloud services. Make sure that the information is secured or, preferably yet, that the documents and information are stored locally, out of the reach of hackers. Avoid generic plug-and-play features: (1) Most IoT systems offer a Standard Plug & Play functionality that enables multiple gadgets to

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

communicate with one another. This eliminates the need to configure each device individually. (2) Though this clearly benefits the Internet of Things setting in the workplace or at home, it needs to have proceeded with caution. (3) To connect Universal Plug & Play standards, local connections are utilized. (4) As can be seen, these systems are susceptible to external attacks and easily exploited. (5) If the attack succeeds it has the potential to affect a massive amount of IoT devices by enabling hackers to manipulate them from a faraway place.

F. Utilizing a backup network

Wi-Fi customers may create many networks and restrict their access to themselves or their contacts. This way of establishing a secondary connection is suitable for IoT devices since it facilitates data collection. (1) Prevent unauthorized access to sensitive data. (2) Stop any attempts to gain control of IoT devices as well as install malware. (3) Completely separate the IoT system from the external environment, securing sensitive data. (4) Ensure that the IoT gadget is regularly updated. Automated renewals are necessitated in order to search for authorized updates from the system vendor, as indicated as a possible IoT security risk. This process installs software patches to electronic or computer devices, preventing intruders from penetrating them.

VI. CONCLUSION

This paper suggests implementing a multi-layered data protection strategy for IoT frameworks for dealing with desktops, documents, online, and internet IoT applications and services, in addition to dealing with risks and concerns as they arise. It was understood that inadequate security in IoT systems could lead to equipment malfunctions, losses, and sometimes even total system collapse. Incorporating security by design ensures that security protocols are adjusted to the most secure settings throughout all stages, especially prior, during, and then after production offering integrity while providing readily interactive IoT data, contents, and applications.

REFERENCES

[1] Bhargava, Akansha, Gauri Salunkhe, Sushant Bhargava, and Prerna Goswami. "A Comprehensive Study of IoT Security Risks in Building a Secure Smart City." Digital Cities Roadmap: IoT-Based Architecture and Sustainable Buildings (2021): 401.

[2] Borovska, Plamenka, and Desislava Ivanova. "In silico knowledge data discovery in the context of IoT ecosystem security issues." In AIP Conference Proceedings, vol. 2333, no. 1, p. 030004. AIP Publishing LLC, 2021.

[3] Da Xu, Li, Yang Lu, and Ling Li. "Embedding Blockchain Technology into IoT for Security: A Survey." IEEE Internet of Things Journal (2021).

[4] Frustaci, Mario, Pasquale Pace, Gianluca Aloi, and Giancarlo Fortino. "Evaluating critical security issues of the IoT world: Present and future challenges." IEEE Internet of things journal 5, no. 4 (2017): 2483-2495.

[5] Gilchrist, Alasdair. IoT security issues. Walter de Gruyter GmbH & Co KG, 2017.

[6] Gou, Quandeng, Lianshan Yan, Yihe Liu, and Yao Li. "Construction and strategies in IoT security system." In 2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing, pp. 1129-1132. IEEE, 2013.

[7] V. Mohan & S. Senthilkumar, "IoT based fault identification in solar photovoltaic systems using an extreme learning machine technique", Journal of Intelligent & Fuzzy Systems, vol. 43, no. 3, pp. 3087-3100, 2022. DOI: 10.3233/JIFS-220012.

[8] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." In 2015 IEEE world congress on services, pp. 21-28. IEEE, 2015.

[9] Kamble, Ashvini, and Sonali Bhutad. "Survey on Internet of Things (IoT) security issues & solutions." In 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 307-312. IEEE, 2018.

[10] R. Manivannan, S. Senthilkumar, K. Kalaivani, N. Prathap, "Performance Enhancement of Cloud Security with Migration Algorithm for choosing Virtual Machines in Cloud Computing", Engineering Research Express, Vol. 6, No. 1, 015204, 2024. DOI: 10.1088/2631-8695/ad2ef9. IF: 1.7, ISSN: 2631-8695.

[11] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[12] Kumar, Vinod, Rakesh Kumar Jha, and Sanjeev Jain. "NB-IoT security: A survey." Wireless Personal Communications 113, no. 4 (2020): 2661-2708.

[13] Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. "Internet of things (IoT) security: Current status, challenges and prospective measures." In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336-341. IEEE, 2015.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.524| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707286 |

[14] Mohanta, Bhabendu Kumar, Debasish Jena, Utkalika Satapathy, and Srikanta Patnaik. "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology." Internet of Things (2020): 100227.

[15] R. Manivannan, S. Senthilkumar, T. Senthil Kumar, “Improved Restricted Boltzmann Machine-based Optimization Model for the Network Security System in Cloud Environment”, Engineering Research Express, Vol. 6, No. 2, 025313, 2024. DOI: 10.1088/2631-8695/ad3f77. IF: 1.7, ISSN: 2631-8695.

[16] Parmar, Monika, Neeraj Kumar, Harsimran Jit Kaur, Abha Sharma, Sandhya Sharma, and Mamatha Sandhu. "Analysis and Comparison of Different Blockchain Algorithms in IoT Security." In IOP Conference Series: Materials Science and Engineering, vol. 1022, no. 1, p. 012059. IOP Publishing.

[17] Patnaik, Ranjit, Neelamadhab Padhy, and K. Srujan Raju. "A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges." In Intelligent System Design, pp. 723- 730. Springer, Singapore, 2021.

[18] Riahi, Arbia, Yacine Challal, Enrico Natalizio, Zied Chtourou, and Abdelmadjid Bouabdallah. "A systemic approach for IoT security." In 2013 IEEE international conference on distributed computing in sensor systems, pp. 351-355. IEEE, 2013.

[19] Saha, Himadri Nath, Reek Roy, Monojit Chakraborty, and Chiranmay Sarkar. "IoT-Enabled Agricultural System Application, Challenges and Security Issues." Agricultural Informatics: Automation Using the IoT and Machine Learning (2021): 223- 247.

[20] Zhang, Zhi-Kai, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. "IoT security: ongoing challenges and research opportunities." In 2014 IEEE 7th international conference on service-oriented computing and applications, pp. 230-234. IEEE, 2014.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com