IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN OVERVIEW OF IOT SECURITY DEVELOPMENTS AND ISSUES (INTERNET OF THINGS)

Dr. A. NITHYA RANI [1]
Associate Professor,
CMS College of Science and Commerce Chinnavedampatti,
Coimbatore.

Ms. BASIL BABY K [2]
Ph.D, Research Scholar,
CMS College of Science and Commerce Chinnavedampatti,
Coimbatore.

ABSTRACT : The Internet of Things is based on the concept of layered design. A range of technologies are used by each tier for information transmission, capacity, and preparation. This study aims to assess the present Internet of Things architecture with respect to the risks and vulnerabilities associated with IoT-enabled devices, as well as potential assurance procedures in light of equipment limits and novel information transfer methodologies. We then discuss IOT applications and architecture. A list of successful real-time IOT applications now in use is as follows: Emerging technologies include things like self-driving cars, smart grids, traffic management systems, logistic management hierarchies, environment monitoring, building safety applications, and many more.

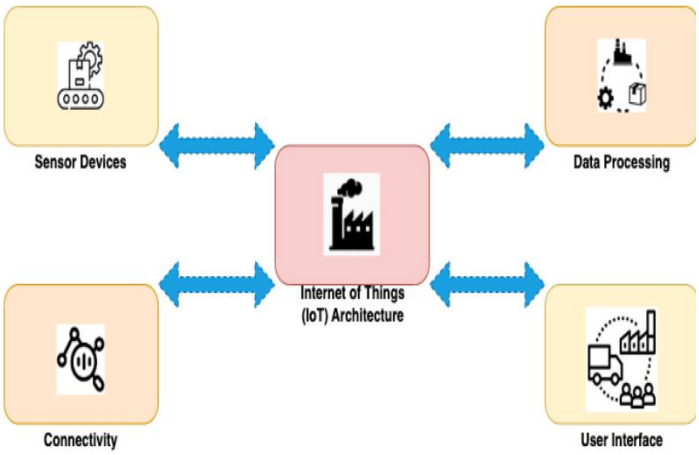
Keywords: Healthcare, Wireless Sensor, application, communication delay.

1.INTRODUCTION

In every industry, the Internet of Things has the potential to drastically change how companies produce commodities and how consumers spend money on management and goods [1, 2]. The Internet of Things promises to fundamentally change the way we create, just like internet services and personal computers did before them. When paired with extensive information research and worldwide broadband communication systems, IOT devices have the potential to improve flexible chain productivity and decrease asset usage while also improving the type of items offered [3]. The Internet of Things is starting to upend the operational and economic frameworks of new industries such as assembly and farming [4].Considering the extensive range of anticipated applications and device types, from simple sensors that passively monitor a situation to complex systems such as autonomous vehicles navigating the world's highways, the Internet of Things (IOT) is poised to introduce new demands and consistency to an increasingly chaotic world [5, 6]. The IOT facilitates innovative ways to bridge the digital and physical realms; however, the landscape of cybersecurity threats is expanding [7]. Digital threats are no longer confined to critical business data or systems, which have traditionally been the focus of organizations' cybersecurity investments; hackers are also targeting devices beyond conventional boundaries [8]. The rapid proliferation of IOT devices, along with their diverse functionalities, significantly increases potential vulnerabilities [9]. Furthermore, the impact of numerous compromised devices becoming active on the Internet, or individual devices affecting the physical world, highlights the growing challenge to cybersecurity practices [10]. It is

imperative for organizations to reassess traditional threats and management strategies in light of this evolving threat landscape [11].The Internet of Things (IOT) refers to a system or process involving interconnected devices that can be controlled via a network [12, 13]. These devices may be mechanical or digital machines capable of operating over the internet without the need for human intervention. Broadly speaking, IOT includes all entities that function through the internet utilizing sensors and transmitting data through cloud networking. Nevertheless, the advent of Blockchain Technology offers a comprehensive solution for enhancing infrastructure security. Recently, many organizations have begun transitioning to this platform to safeguard their data, despite the complexities of intercommunications [8,9,10,11,12,13,14,15,16,17,18,19,20,21]. The operational aspect of IoT is linked to the cloud [14]. An IoT system is composed of sensor-based devices that communicate with the cloud through connectivity. Once data is collected, the software processes it and executes the desired action as specified by the user. If user input is required, the system captures this input through the user interface, and any necessary changes are communicated to the cloud. Subsequently, the updated data is relayed back to the sensors or devices capable of executing the user's requested action [15]. The IoT framework is built upon four primary components that facilitate its operation, as illustrated in Fig. 1:

- Sensor devices
–Connectivity
-Data processing
-User interface



1.1 SENSOR DEVICES

A sensor is a small microchip embedded in devices that sense or collect environmental data [16]. It could be as simple as reading the temperature or collecting a bundle of information as collecting video data. For example, let us consider the mobile you use daily. The mobile contains sensors like a GPS controller, camera, gesture reader, etc.

1.2 CONNECTIVITY

The second thing comes, which is essential, which is connectivity. The sensor needs a connection to the cloud for communication, like 5G. For this, several methods have been used depending on the hardware and the types of devices the user sets [17]. They can include cellular, Wi-Fi, GPS, satellite, LAN, WAN, or any connection. Each connection has limitations and bandwidth, so the user has to choose one of the better options for their relationship.

1.3 DATA PROCESSING

The data gets to the cloud, so the software in the application performs some kind of processing on it, such as checking the temperature in a reasonable range and the house activity through cameras [18].

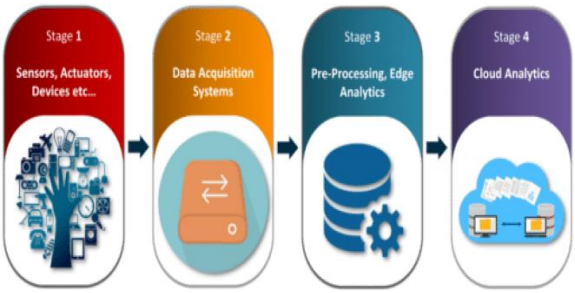
1.4 USER INTERFACE

In the IoT framework, the user interface is crucial in managing IoT applications. Some rules are defined for the user [19]. For example, if the temperature is too high, an alert or message is sent to the user to check the temperature and set the environment. But in some contexts, there is also an automatic system available that checks the temperature, and on high alert, it automatically performs some actions and controls the condition, and it depends on the applications used in the IoT framework [20].

2 IOT ARCHITECTURE

IoT is not just an internet-connected device; it is the technology IoT is the technology that builds a system capable of sensing and responding to the world without any human intervention. The IoT is generally working into four stages given in Fig. 2 (also discussed in Table 1); these stages are:

1. i.Sensors and Actuators Devices
2. ii.Internet Gateway and Data Acquisition System
3. iii.Pre-Processing Edge IT
4. iv.Cloud and Data center



2.1 Sensors and actuators devices

The first layer of these four stages is called Sensors and actuators [21]. The sensor collects data from an environment and converts it into usable data [22]. Smartphones are an example of this stage. Smartphones contain sensors that detect the earth's gravitational, allowing them to orient their screen depending on your position. Actuators are devices that can intervene in the physical reality that generates data—for example, shutting off an engine, switching off the light, and adjusting the room temperature. These Senses and actuating stages help to adjust everything in the physical world and for information that requires deeper insight for more analysis. The data must be collected in a cloud-based system, as mentioned in Table 1. There is some sensors type applied in IoT.

- Temperature Sensors
- Moisture IoT Sensors
- Light IoT Sensors
- Water Level IoT Sensors
- Image IoT Sensors

2.1.1 Temperature sensors

These sensors are found in every IoT case keeping track of the thermal condition of air, environment, machines, and other objects [23]. Temperature sensors are helpful in manufacturing warehouses, plantations, weather reports, and agriculture, where the soil temperature is highly monitored to balanced and provide maximum growth [24].

- *Thermistors*: Its resistance depends on the temperature. It's mostly used in electronics like an electronic thermometer.

2.1.2 Moisture IOT sensors

Widespread uses in the metrology station to report forecast weather, moisture, and humidity sensors are also employed in agriculture, food supply chain, and health monitor system [25].

- *Hair tension Moisture System* It is the oldest type of moisture sensor based on human and horsehair or cotton fiber. The fiber or hairs change their length upon contact with moisture. Pointer the reading on scale and connect with hair and fiber. These moisture sensors are cheap construction [26].

2.1.3 Light IOT sensors

Light sensors depend on the light intensity, and these are easily found in smart TV, Mobile phones, and Computer LEDs through up and down the brightness [27].

- *Photo resistors*: Its resistance changes through radiation because it's a photosensitive element. It is easily connected via analog light sensors. Lamps are an example of a photo resistor it turns automatically turn after Dark.

2.1.4 Water level monitoring sensors

Water level monitoring sensors are used in flood warning system for prediction and environmental protection in case any natural disaster is coming so it can send a warning [28].

- Optical Sensors: a sensor that detects water level by the reflection of light in the prism.

2.1.5 Image sensors

Image IoT Sensors are used whenever the need for the smart devices to look the happening in the surrounding it used in security systems and military equipment, and other things [29].

- Active Pixels Sensor: DSLR, webcams, Digital X-Ray is an example of active pixels sensors.

Actuators are separated in four categories.

- Linear: Motion of object and element in straight line.
- Motors: Rotational Components and whole object
- Relays: Electromagnet Based Actuators
- Solenoids: used in home appliances.

2.2 Internet gateway and data acquisition system

Data from the sensor come in analogue form, so it must be converted into digital form; the Data acquisition system (DAS) is the tool to aggregate and convert it into digital format. It could happen in the 2nd stage of IoT architecture, called internet gateway [30, 31]. Data acquisition devices help machines more innovative analyze actual data. It is used in industrial and commercial electronics and environmental and scientific equipment to capture signals and environmental conditions.

Data acquisition consists of:

- Signal Condition
- Recorder and Display Devices
- Data handling
- Multiplexing
- Transmission and storage
- *Signal Condition*: Output signals of transducers are very weak signals which cannot be used for further processing [32]. Various types of signals conditioner are used to make the signals strong, like filters AND Modifiers.
- *Multiplexing*: Accept multiple analog inputs and provide a single output signal according to the requirement.
- *Display Devices*: Data is displayed in a suitable form to monitor the input signals like Oscilloscopes, Numerical Display, and Panel Meter. Data can be permanently or temporarily stored and recorded in Optical or ultraviolet recorders.

2.3 Edge IoT

It is the 3rd Stage of IoT Architecture. The prepared data is transferred to the IT World [33, 34]. This stage is closely linked to the previous Phases of IoT Architecture stages, sensors and actuators, because the location of the edge system is located where sensors and actuators are located. Edge devices in IOT can also benefit from high-class IoT projects. It provides high speed in data transfer cloud platforms and performs faster response time and extra flexibility in data processing. There are Some Components of Edge Computing in IoT, as mentioned in Table 1.

- Machine learning (ML) and Artificial Intelligence
- Complex Event Processing (CEP)
- Machine Learning (ML) and Artificial Intelligence:

The Idea of Machine learning Models are built by Using complicated, so it turns into artificial intelligence AI. Most edge IoT devices support machine learning ML models [35]—some Edge devices are Delivered directly to IoT Devices.

- Complex Event Processing:

Complex and Event Processing (CEP) Services and Software are used in several Operational technologies [36]. CEP takes data from multiple sensors and acts on a specific platform. CEP and Pattern Models push edge devices. The most common technology is the Apache storm.

2.4 Cloud and data centre

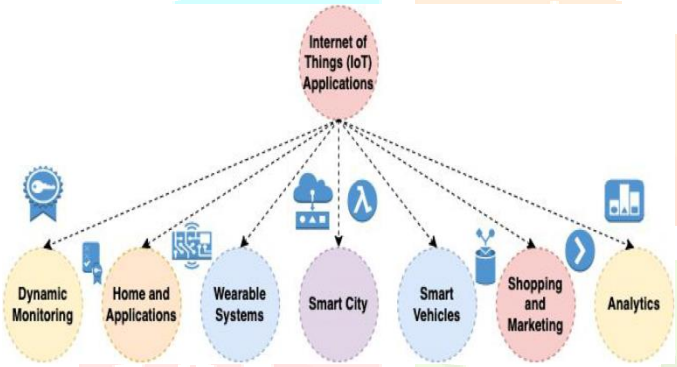
It is the 4th stage of IoT architecture. The primary process happens in the data center and cloud [37]. It makes the system more secure and robust IT System. There are some stages in the cloud.

- *Cloud Discovery*: it helps data stored inside the on-premise or data warehouse.
- *Cloud Data Migration*: In this system, you need to decide on what type of data load into the cloud, how more efficient is.
- *Cloud Data Maturity*: At this point, you are ready to make the harder cloud work and hone your cloud data management strategy. Cloud data

Maturity technology is the second nature of data professionals [38]. But right now, you have made solid type cloud data use in cases, improved analytics, and reporting for part of the business.

3 IOT APPLICATIONS

IoT's motive is to bring changes to our life for the betterment. With new wireless networks, revolutionary computing capabilities, and superior sensors, the IoT will hope to become a frontier in the race and share of the wallet. At the same time, some needless about the current hype about IoT is the biggest. Nowadays, many companies announce prediction IoT-based devices, and we discuss a significantly trending IOT app right now [39] and also given in type in Fig. 3.



3.1 Smart Home A smart home represents one of the most prominent examples of an Internet of Things (IoT) application [42]. Monthly searches for smart homes on the Internet reach approximately 60,000 [43]. Currently, over 256 companies are engaged in the smart home sector, making it a significant area within the IoT landscape [44]. The investment in smart home startups is estimated to be around $2.5 billion. Notable names in this industry include Alert Me and Nest, along with several multinational corporations such as Samsung and Apple. 3.2 Smart City A smart home is also recognized as one of the leading applications within the IoT domain. This concept encompasses a wide range of functionalities, including waste management, traffic control, environmental monitoring, and water distribution. The appeal of this term lies in its potential to address the major challenges currently faced by urban areas [45]. Additionally, it contributes to the reduction of noise and pollution, playing a vital role in assisting cities.

3.3 Smart Grid A smart grid is recognized as one of the most effective applications for the Internet of Things (IoT) [46]. The forthcoming smart grid is expected to automatically gather data regarding the behaviors of electricity consumers and suppliers, thereby enhancing efficiency and reliability [47]. Additionally, it is noteworthy that the concept is projected to achieve approximately 41,000 searches on Google [48]. Conversely, the volume of tweets related to this topic is around 100 per month, indicating that people either lack interest or have nothing to contribute regarding it.

3.4 Car connected: The advancement of connected cars is progressing at a gradual pace. Based on current trends, it is suggested that the automotive industry typically undergoes a cycle of about 3 to 4 years; however, there has been little evidence of developments in car connectivity. Some entrepreneurial startups are engaged in projects related to connected cars, which is a positive indication for this initiative. Notable corporations such as Apple, Microsoft, and Google have announced their ventures into connected vehicles [49,50,51].

3.5 Health connected Connected health is often regarded as the untapped potential within IoT applications [52]. When discussing intelligent medical devices and connected healthcare systems, their potential is immense, benefiting not only organizations but also individuals. To date, advancements in this area have been limited, primarily driven by specific use cases and startups; the broader scale of implementation remains to be realized.

3.6 Supply smart chain It is widely acknowledged that the supply chain has been increasingly intelligent for several years. The ability to track goods in transit and facilitate the exchange of inventory information among suppliers has been established for many years. Predictions suggest that the integration of IoT will further enhance this intelligence. Currently, its popularity appears to be on par with that of smart home technologies [53].

3.7 Industrial net The industrial internet represents another significant application of IoT. Various market research entities, including Cisco, recognize the industrial internet as an IoT concept with substantial potential; however, its popularity has yet to reach the widespread acceptance seen with wearable technologies [54].

3.7.1 Wearable The topic of wearable's is currently experiencing significant popularity. As a consumer, you have been eagerly anticipating the launch of Apple's new

smart watch. There is a wealth of innovative wearable technology to look forward to, such as the Look see bracelet [44]. Among the leading startups in this field, Jawbone stands out as one of the most well-funded, having raised approximately 500 million US dollars! [55].

3.7.2 Personal assistance We have been accustomed to smart phone assistants for many years; now, this technology has expanded into smart homes, exemplified by Amazon's well-known personal assistant, Alexa [56]. This personal assistant enables us to manage our smart home both digitally and virtually [57].

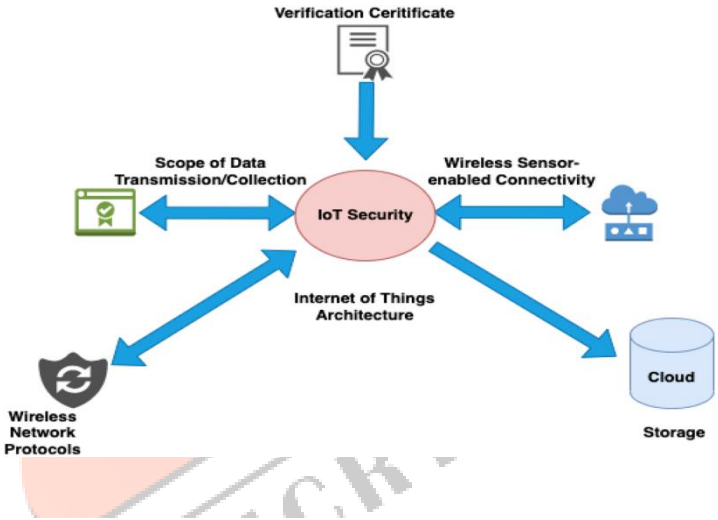
3.7.3 Video doorbells :Another cutting-edge advancement in IoT is the video doorbell. These devices allow users to respond to calls from the video doorbell when someone arrives at their door. They also provide the capability to lock and unlock homes via a smart phone application. An additional feature is the ability to notify homeowners when someone is moving around the property, and users can set specific times during which notifications or alerts are disabled [58].

3.7.4 Smart Locks: In the contemporary world, the crime rate is escalating daily due to factors such as poverty and theft, among others. During this period, smart locks emerged as one of the cutting-edge technologies in smart homes. With this technology, we can conveniently lock our doors using a mobile application, whether we are at the office, in a car, or anywhere else.

3.7.5 Traffic Monitoring: The Internet of Things (IOT) plays a significant role in traffic monitoring and management, proving beneficial for us as it regulates traffic in smart cities. When we activate the sensor on our smart phone during our journey, it collects data and transmits it to our vehicle via applications like Google Maps. This provides us with information and displays various routes along with current traffic conditions. After analyzing all available routes, it suggests the optimal path with the least traffic and informs us of the estimated time of arrival, distance, and destination. 3.7.6 SmartWatches:Smartwatches represent another instance of IOT technology. These devices not only tell time but also monitor heart rate, pulse, calories burned, timers, and the number of steps taken while running or walking. While smart watches provide this information, they also require a compatible smart phone with an application that pairs with the watch. Through this mobile application, we gain access to our smart watch, which operates based on sensors and the interconnectedness of IOT[61,62,63].

4.CATEGORIES OF IOT SECURITY

The number of applications connected through the Internet over the year and the ratio is very high. The report says that almost 30 billion devices connected will mark through the Internet and 75 billion onwards to 2025 [64]. So, the ratio of the number of devices is more than we expected, so for a better experience by the user, we have to do our best in security for the application. Thus, to protect these devices and to reduce cyber-attacks and hacking problems, as shown in Fig. 4;



4.1 Risk Categorization

Deciding the appropriate level of security restrictions for a specific item or service depends on its associated risk profile. For obvious reasons, a threat with a potential fatal impact necessitates a higher level of security than the risk posed by a compromised asset following a label on a tube of toothpaste [66]. However, rather than focusing solely on inconsistent outcomes, it is more prudent to consider specific IOT devices in relation to their use cases and management [67]. To establish security levels, utilizing risk classifications, discussions, and decisions helps eliminate the potential for inconsistencies in security strategies. It also provides a means to develop templates and tools that organizations can use to make the application of IOT security restrictions, policies, and procedures more consistent. Risk classifications can reduce the ambiguity involved in creating security prototypes for an increasingly diverse and interconnected landscape of products and services [68]. A crucial first step in categorizing IOT risks

is to define them. Broadly speaking, the IOT transformation is driven by the anticipated consequences of a compromised device, whether they are operational, managerial, physical (health and safety), or tangible. IOT risk varies significantly by deployment and differs somewhat from traditional Information Technology threats, which have focused on preventing network breaches and data exfiltration from beyond the corporate firewall. The IOT also differs greatly from traditional Information Technology due to its networking model [69].Many corporate IT infrastructures are designed as semi-private networks with minimal exposure to the external world, particularly the Internet. The security of the network is typically enforced at the network boundaries and on the internal endpoints, such as Personal Computers and connected printers, by monitoring and preventing inbound attacks [70]. Established best practices and technologies are readily available to help organizations mitigate these threats. A variety of security breaches are linked to the layers of IOT; each layer is susceptible to different types of security attacks [71]. These attacks are often unique or isolated and are frequently initiated by either an internal or external source [72]. A dynamic attack will immediately disrupt the network, while a passive attack can extract data from the IOT system discreetly without interrupting the network. DOS attacks can affect every layer of IT, rendering the network services unavailable [73]. In this section, we will examine the security issues associated with each layer of IOT.

4.2 Perception layer

The perception layer of IOT is the most sensitive, where most attacks are launched; the centers on this layer by and massive include external conditions, which makes it the most adored attacking region in IOT orchestration [74]. Distant development is used to send the sign between the centers of IOT; like this, its adequacy is typically reduced by waves disrupting impact. Recognitions to the surface sending of the IOT sensors, an attacker can adjust the gear of the devices [75, 76]. Also, the devices on the perception layer include sensors, scanner label peruses, or RFID, whose estimation limit and power use are extraordinarily low, which makes them attackable. Evaluating is regularly used to abuse the mystery of this layer, which may exchange character information about IoT devices. The center catch attack can be prepared on this layer, during which the attacker expects command over the center point and focuses all the data from the center point. Moreover, the attacker can change center points on this layer.

4.3 Network layer

DOS attacks are frequently executed viably on the network layer [77]. Inactive watching and framework inspecting are furthermore ordinary on the network layer. Transferring data from devices and a neighborhood of remote access offers an increase in those sorts of attacks [78]. Just in case a spy can grow the entering material of IOT devices, secure correspondence is getting to tend up around then. An appropriate segment of crucial exchange should be guaranteed for the secure communication of IOT devices [79]. The communication between the IOT devices is almost the same because of the web; the rationale is that it's not confined to machines but to humans. The likeness is that the significant issue for the security of IOT devices, as a consequence of the heterogeneity of the IOT devices at these available shows, cannot be used. The range limits need to, in like manner, be extended to shape IOT devices sufficiently prepared to influence any particular condition which may impact their security.

4.4 Application layer

There are no overall standards and courses of action for advancing IOT applications; there are various security issues related to IOT applications [80]. There are multiple applications, and every application has a unique procedure for approval, making it hard to ensure affirmation and security. The growing number of related attackers sharing knowledge will cause an overhead. This overhead will cause the unavailability of IOT organizations. Throughout the application development pattern, another problem must be seen as that's who is getting to be the machine's customer and thus the way they accompany the devices. There should be a few expenses for the purchasers that they are getting to be used to control the knowledge and to infer what data should be revealed and who are getting to be the customer of knowledge once they go to use the knowledge.

5 IOT SECURITY CHALLENGES

As more actions handle the IOT, an enormous gathering of new security faults will arise. The extended risk can be recognized to create restrictions and failed opportunities to improve security. Here are driving IOT security challenges that try must address.

5.1 The rise of botnets

In recent years, there has been an arose of botnets between IOT devices; when botnet exits when hackers remotely control IOT devices by accessing through a vulnerable port and then controlling them, and then they are for illegal purposes, the decentralized organization could enable and choose them as part of a botnet. Still, the main problem is that many companies need more -real-time security to track the hacker [81, 82].

5.2 More IOT devices

In the recent 2000 or a few years ago, the professional was mainly focused on completely protecting mobile devices or computers, but now there is a conflict of IOT devices. well, a recent survey tells that there are over 7 billion devices across the world and that number is increasing day by day and is going towards 20 billion by 2020, so that main problem is that more IOT devices mean more security issue and that why it challenges for the security professional [83].

5.3 Brute forcing/default password

The Mirai bot is mostly used in some of the biggest and most distributed DDOS attacks, and because of that some issues arises when shipping devices with default passwords and intentionally not telling the consumer to change the password as soon as they receive it, there some government which do not permit manufacturers to sell devices with default password like admin as username and same as password [84]. Why Mirai vulnerability was so in working because it identifies the vulnerable devices and uses default credentials and then infects them.

5.4 Malware and ransom ware

As you know, the number of IOT-connected devices is rising, so malware and ransom ware use to exploit them; ransom ware entirely relies on encryption and locks out the user of gadgets. A merge of malware and ransom ware creates a wholly new type of attack and hybridization [85]. Ransom ware attacks could focus on limiting the traffic flow, disabling device functionality, and stealing user data.

5.5 Botnets aiming at crypto currency

Due to the popularity of crypto currency, there is also an increase in the craze of hacking to get crypto cash; new technology such as block chain has been launched to avoid hacking, but there is still a problem in app development using block chain, which is running itself [86]. Different methods are used to extract credentials, but social engineering is common. Many users use VPN to divert IP and video cameras to mine crypto, such as the open-source monero, which is a digital currency mined with IOT devices.

5.6 Home invasions

The scariest is that IOT is mainly installed in houses, and it causes home invasions because of web connectivity and its use in home automation. The security of these IOT devices is a big problem as they can expose your IP address and pinpoint it; the most precious information cans old to hackers on the dark web, and they use it to blackmail another when you are using IOT in your security system. There is a chance that it will leave houses at the exploitable level [87].

5.7 Remote vehicle access

Apart from home threats, there is a chance hijack of your car is a threat. Some car technologies are on the verge of becoming a reality by connecting to IOT devices, and it is associated with IOT; hackers can have control of your car by accessing it, and it is a lethal vulnerable [88].

5.8 Lack of encryption

Ignoring the way that encryption is an extraordinary strategy to shield developers from getting to data, it is, moreover, one of the primary IOT security challenges [89]. These devices do not have the limit and deal with capacities that would be found on a standard PC. The result is a development in traps where software engineers can, without a remarkable stretch, control the estimations expected for protection. But encryption won't be a security asset if an undertaking settles this issue.

4 CATEGORIES OF IOT SECURITY

Technological advancement also produces security solutions as some people use it to spread negativity. The increase in the demand for IOT applications makes sense because it has a vast concept, as it has raised many security issues related to privacy issues, unauthorized access, cyber-attack, and data hacking [98]. Many security experts use strong passwords and other tricks to save IOT devices. However, hackers can exploit many loopholes to gain remote access and steal the data of the user or the device.

The increase in cyber threats in the IOT application and devices gives importance to and highlights the issue that some essential practices should be made to solve these problems [99]. The DOS attack and many server attacks open the window that security issue is more accurate for IOT applications. So many solutions are provided by experts and other security agencies to protect user identity and data.

6.1 LOWPAN security

IEEE 802.15.4, Specification for Low-Rate Wireless Networks, is the basis for Low-Power Wireless Personal Area Networks. The standard is introduced with many systems, including LOWPAN, ZigBee, Z-Wave, EnOcean (State Protocols for Building and House Automation) and SNAP [100]. IPV6 and IEEE 802.15.4 merge the concept of LOWPAN. The home automation systems thread protocol even reaches LOWPAN [101]. One or more of the LOWPAN networks, the edge router, which regulates the entry and performance of the LOWPAN, are linked to the Internet. In the configuration of the RPL, routing problems in 6LoWPAN are discussed by the IETF-ROLL task force. The protection in the LOWPAN networks must only restrict access to records for approved users, maintain data integrity, and prevent malicious intruders. To track traffic on both sides, an intrusion detection system is needed. The lack of encryption at the 6LoWPAN layer, optimum semiannual effort on fracture connections, and restricted networked system memory make LOWPAN's packet fragmentation framework vulnerable.

6.2 Security in RPL

In low-power networks deployed over 6LoWPANs with high or inconsistent packet loss mounts, IPv6 Routing Protocol for LLN (RPL) is designed for routing IPv6 traffic [102]. A “Security” field after the ICMPv6 message header is used for RPL protection. In this area, information indicates the security level and encryption algorithm used for message encryption. LDR provides data authentication support, somaticized security, replay protection, and critical management. The selective transmission, sinkhole, Sybil, hello-inundations, hyperspace, black hole, and denial of service attacks are used in RPL attacks.

6.3 Security in bluetooth low energy

6.3.1 BLE protocol

BLE is a low-performance version of wireless Bluetooth 2.4 GHz. Although classic Bluetooth BLE signal strength and radio range are smaller than specific metrics, BLE is designed to run on a copper battery (e.g. the common CR2032) for high-power applications [103]. BLE sensor devices can run for several years without needing a new battery, thanks to their low power and long battery life. The latest BLE Secure Connections model is implemented in BLE version 4.2 to improve protection. Review the main security issues of BLE: passive rescue.

6.3.2 Eavesdropping

Passive eavesdropping defense can be used by encryption [104]. BLE 4.2 uses Elliptic Curve Diffie-Hellman (ECDH) algorithm for data encryption. In contrast, earlier versions of the BLE (Bluetooth 4.1 or older) apps used the easily guessed partial key for the first time to crypt a connection.

6.4 Identity tracking

Third-party devices that are connected with addresses and provide device authentication of the devices that transmit the information and monitor the users. A regular change of private addresses to defend against this thread only the trusted parties can overcome them [105].

6.5 Zigbee security

Zigbee security requires the presumption of safe stocking of keys and the pre-loading of computers with symmetrical keys so that they will not be transmitted unencrypted. This unique unprotected critical transmission provides a short

operating time frame, during which an assailant can sniff the key [106].

6.6 RFID security

The classification of radiofrequency is the way to classify the "people" uniquely by using radio waves to transmit their identity (usually a serial number). At least one RFID device is composed of a tag, an antenna, and a scanner. RFID tags are connected to read devices using the RFID reader to store identifications and data. Active, passive, or passive-aided RFID tags may be. Active RFID tags can be distributed with readings ranging up to 100 m. Battery-free devices can use passive tags, as the ID is read by the reader passively. You have a read distance of up to 25 m from close touch and use the strength of an interrogating reader for all responses [107].

7 OPEN RESEARCH ISSUES

The IoT technology is in the development phase and needs to mature more, so less user knowledge, poor maintenance, and updates and development standards are problems for security [108]. IoT devices have weak security, or user unaware of security measures that a hacker will easily control by using malware for ransom [109]. The control of IoT devices harms wearable devices, smart homes, and health-related applications. If the ransom is not paid to the hacker, then IoT-based vehicles will not start, or the locked homes will not open, so still, research is required in this area to make more secure IoT devices from this type of attack.

8 CONCLUSION

The main worry when using IoT devices is security rather than any problems with the devices themselves. However, the primary factor bringing attention to the problem of security lapses—the reason we encounter attacks on a daily basis—is the data on the internet. IoT gadgets, on the other hand, will be the most important technological innovation in 2020 and beyond since they make things easier by using the internet and efficiently completing household tasks. In this work, we review and classify security vulnerabilities based on their type and frequency of occurrence, such as malicious attacks, malicious insiders, etc. We also go over the available solutions and how they help secure IoT devices. Additionally, we offer open research topics for future advancement in order to help organizations and researchers address security-related problems.

8 REFERENCES

1. Yin S, Li H, Laghari AA, Gadekallu TR, Sampedro GA, Almadhor A. An anomaly detection model based on deep auto-encoder and capsule graph convolution via sparrow search algorithm in 6G Internet-of-everything. IEEE Internet Things J. 2024.
2. Fatima Z, Rehman AU, Hussain R, Karim S, Shakir M, Soomro KA, Laghari AA. Mobile crowdsensing with energy efficiency to control road congestion in internet cloud of vehicles: a review. Multimed Tools Appl. 2023;83:1–26.
3. Sony M. Industry 4.0 and lean management: a proposed integration model and research propositions. Prod Manuf Res.
4. Yahya N. Agricultural 4.0: its implementation toward future sustainability. In: Green Urea. Singapore: Springer; 2018. p. 125–45.
5. Jeong YN, Son SR, Jeong EH, Lee BK. An integrated self-diagnosis system for an autonomous vehicle based on an IoT gateway and deep learning. Appl Sci. 2018;8(7):1164.
6. Gao J, Li P, Laghari AA, Srivastava G, Gadekallu TR, Abbas S, Zhang J. Incomplete multiview clustering via semidiscrete optimal transport for multimedia data mining in IoT. ACM Trans Multimed Comput Commun Appl. 2023;20:1–20.
7. Jardine E. Mind the denominator: towards a more effective measurement system for cybersecurity. J Cyber Policy. 2018;3(1):116–39.