JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

INTERNET OF THINGS IOT SECURITY: THREATS & CHALLENGES

[1]Sanjay Srivastava, [2]Dr.Manish Varshney

[1]Research Scholar, Department of Computer Science, Maharshi University of Information Technology, Lucknow [2]Professor, Department of Computer Science, Maharshi University of Information Technology, Lucknow san.sri2k@gmail.com, manishv@muit.in

ABSTRACT

The Internet of Things (IoT) revolutionized the global network comprising of people, smart devices, intelligent objects, information, and data. It is no secret that as more and more devices connect to the internet, the challenges of securing the data that they transmit and the communications that they initiate are becoming more profound. In this century of automation, automation, which is digitized and more and more technology is applied, makes people's lives easier. When individuals feel unsafe on the Internet, they are less likely to use it, which is the situation currently. When it comes to gadgets and sensors, the "Internet of Things" IoT has made this possible. There has been an increase in the production of compact, low-cost sensors as a result of advances in sensor technology. Temperature, pressure, vibration, sound, and light are a few examples of sensors that may be utilized in the Internet of Things. Increasingly powerful IoT applications are being developed as a consequence of the continuous improvement of IoT sensors with each new generation. As a result, discussing their security concerns and risks might be difficult. There are several advantages and disadvantages to IT applications that are discussed in this article. One- hundred-and-ninety-nine percent of the papers analyzed considered cost the most important consideration when assessing IoT applications, followed by real-tameness (64 percent) and security and error (57 percent). DDoS assaults, an in-depth look into DDoS assaults on IoT devices, the consequences of DDoS attacks, and mitigation methods are presented in this article. Detection models for DDoS assaults are compared in this review article, which focuses on Intrusion Detection models. Also given were several IDS classifications, multiple anomaly detection methodologies, various IDS models created from datasets, and various machine learning and deep learning algorithms for data pre-processing and malware detection. As a result of the discussion on research difficulties, solutions provided, and future aspirations, a larger viewpoint has been envisioned.

KEYWORDS: "Internet of Things"; Industrial IoT; Smart manufacturing; Threats Future technology.

INTRODUCTION

The Internet of Things (IoT) has been one of the fastest developing technology trends in recent years. According to IoT Analytics, by 2025, there will likely be more than 27 billion connected devices in the world. However, increasing security concerns like software vulnerabilities and cyber attacks can make many customers refrain from using IoT devices. Such Internet of Things security problems are especially significant for organizations that operate in healthcare,

Submitted: 16/11/2022 **Accepted**: 05/12/2022

finance, manufacturing, logistics, retail, and other industries that have already started adopting IoT systems.

Many "Internet of Things" IoT applications have profited tremendously from recent improvements in IoT technology, including smart homes, digital health care, smart grids, and smart cities. Statist estimates that by the end of the decade, there will be 75.44 billion connected devices, up from 20.35 billion in 2017. According to the International Data Corporation (IDC), spending on IoT technology is expected to climb from $698.6 billion in 2015 to more than $1 trillion by 2019, meaning that IoT technologies are having a major and increasing impact on our everyday lives. [1]

While IoT applications and devices are growing at an exponential rate, cyber-attacks are also becoming better and represent a greater danger to security and privacy than ever before. Implantable medical devices and smart automobiles might be compromised by distant attackers, which could not only cause significant economic losses but also put people's lives at risk. As IoT devices become more extensively employed in many sectors of business, the military, and other crucial institutions, hackers may pose a threat. On January 31st, 2018, the manuscript was received. The authors of this paper are from the “National Computer Network Intrusion Protection Center” of the Chinese Academy of Sciences in Beijing, China (postal code 100000). On October 21st, 2016, the Domain Name System (DNS) provider Dyn was the target of a distributed denial of service (DDoS) assault, rendering popular websites like GitHub and Twitter inaccessible. Attackers used an IoT botnet, a network made up of printers, IP cameras, gateways and baby monitors to carry out this assault. Stuxnet, a highly advanced computer virus, has caused significant damage to Iran's nuclear programme. [2]

Most businesses and people, on the other hand, are ignorant of the need of protecting their private information. More than half of Americans believe that their personal information has been misused, according to a recent Pew Research Center research. Only 26% of Americans object to the sharing of their medical records with their doctor. In addition, almost half of Americans believed that insurance firms should be They are authorized to monitor their location and speed in order to deliver these discounts on their policies As a result of a lack of

demand from consumers, manufacturers used to focus on the product's fundamental functions while ignoring security. IoT device makers, on the other hand, seldom give out firmware upgrades to their products unless users specifically request them. However, owing to resource constraints, IoT devices often do not execute full-featured security systems. IoT devices typically include easy-to-use vulnerabilities (such as passwords and faults that haven't been fixed) that may be exploited for long periods of time. [3]

There are a lot of companies making IoT devices, cloud service providers, and researchers all working on ways to secure data flow between devices, find new vulnerabilities, and ensure privacy and security for both users and devices. IoT security and privacy are being improved, however many research are still in the early stages and are not practical, therefore many questions remain unanswered. There are a number of published surveys on IoT security in order to bring out significant paths for additional study and give helpful references for researchers. For the most part, Li et al. and Lin et al. spoke about and assessed the present assaults and issues that follow layers. A study by Fu et al. examines the prospects and dangers in the home and hospital settings for two distinct types of applications. [4]

It is necessary to deal with concerns and procedures such as authentication, access control, confidentiality, and privacy in order to keep user data secure. IoT attacks are classified according to Yang and colleagues' current research, which synthesizes the findings of earlier studies. There was a wide range of topics covered, including the latest developments in IoT security, dangers, and outstanding challenges, as well as some suggestions for future study. There are many issues and hazards that IoT presents, but only a handful of them have been thoroughly researched and explained. IoT devices have a number of restrictions, however Yang et al. Only look at the problems caused by limited battery capacity and CPU power. IoT security and privacy may be jeopardized if many additional features and limits are not addressed. [5]

LITERATURE REVIEW

AMIR MASOUD RAHMANI (2022) In this century of automation, automation, which is digitised and more and more technology is applied, makes people's lives easier. In the modern world, the Internet has become an essential aspect of people's everyday life, unless they are unable to protect themselves. As a result of the “Internet of Things” (IoT), devices and sensors may now be linked to the internet and managed remotely. There has been an increase in the production of compact, low-cost sensors as a result of advances in sensor technology. Temperature, pressure, vibration, sound, and light are a few examples of sensors that may be utilized in the Internet of Things. Increasingly powerful IoT applications are being developed as a consequence of the continuous improvement of IoT sensors with each new generation. As a result, discussing their security concerns and risks might be difficult. Benefits, risks, and limits of “Internet of Things” IoT applications are discussed in this study. The cost of IoT applications was found to be the most relevant aspect in 79 percent of all articles, followed by real-tameness (64 percent), and security and error (57 percent) in the evaluation. [6]

KAMRAN SHAUKAT ET.AL (2021) Modern big data is a product of today's new technology, known as the Internet of Things (IoT). Everything should be linked to the Internet under the current IoT paradigm. Since it provides new chances for unique services, IoT presently and unquestionably serves as a platform for future growth. Since the amount of calculations, a computer can do about doubles every two years, the Internet of Things IoT business is booming. When compared, the size and power requirements for the same time period are approximately half. A broad variety of applications may now be achieved by using smaller and more powerful devices for connectivity and data transmission. Because of this, there are substantial security issues that need to be addressed going forward. Healthcare, home automation, smart cars, and other industries are all benefiting from the Internet of Things (IoT). While the Internet of Things IoT offers many benefits, it also introduces new security risks. Security issues, such as safeguarding these devices, information, and communication from those who aren't authorized to access them, are evident. IoT features confront security concerns, and what solutions have been developed so far, and what are the remaining issues.

NIVEDITA MISHRA (2021) everything from education to transportation to healthcare is being transformed by “Internet of Things” IoT technology. IoT technology faces several issues as the number of connected devices raises, including heterogeneity, scalability, quality of service, and security needs, to name just a few. Because of the high cost, limited size, and limited power of IOT devices, security management often takes a backseat. The lack of security makes people wary of utilizing “Internet of Things” IoT devices, which puts them at danger. That means that IoT is prone to security breaches, resulting in huge financial and reputational damages. It fulfils an essential need to examine current security threats and address the issues of the future in order to be prepared for them. Several levels of IoT security have been examined, including the perception, network, support, and application layers; a particular emphasis was placed on Distributed Denial of Service (DDoS) threats. DDoS assaults pose a serious risk to the online world because of the damage they may deliver to their targets. An in-depth look at DDoS attack types, IoT device DDoS assaults, the effects of DDoS attacks, and mitigation strategies is provided. Intrusion Detection and Prevention models are compared in the provided review study, which focuses on Intrusion Detection models. Many anomaly detection algorithms, models for Intrusion Detection System models, and different machine learning and deep learning approaches have also been presented. We've taken a broader look at research concerns, possible solutions, and future goals. [7]

NOSHINATARIQ ET.AL (2021) Internet of Things IoT applications include smart homes, smart cities, smart grids, and smart vehicles. All of these apps use a distributed data delivery system that makes it possible to use them from anywhere in the world. Smart things can communicate with one other, allowing for new ways to increase human well-being. Massive communication in such systems presents a broad range of security issues. However These flaws in security might have devastating implications if they disrupt the whole program or system. As a result, modern IoT applications need a high level of trust and security. Security issues in

smart IoT applications, including e-health, agricultural and energy industries must be well understood. As a result, in order to improve the security of smart IoT applications, this article presents and explores the most important security problems and needs.
RAO FAIZAN ALI (2021) when it comes to technology, the “Internet of Things” (IoT), often known as the “Internet of Everything” (IoE), represents an entirely new paradigm. Information Technology (IT) is enriched by the Internet of Things, which allows devices to connect with other machines and people. Various IoT devices and designs have been developed by researchers and the IT sector. The “Internet of Things” IoT idea is presented in a variety of ways. Security is becoming a major problem as the IoT becomes more prevalent in applications such as smart homes and cities. The purpose of this page is to compile information about documented IoT security vulnerabilities, classifications of those issues, and remedies to those issues. [8]

RAKESH KUMAR SAINI (2019) “revolution in the global network of people and devices, intelligent products, and information and data since the Internet of Things was introduced (IoT). The proliferation of internet-connected devices has made it increasingly difficult to safeguard the data they transmit and the connections they establish. The number of Internet of Things IoT devices has steadily increased over time, particularly in the home and the workplace. We've witnessed a thriving ecosystem around Amazon's Echo devices thanks to the Alexa Voice Service. Several other companies have gotten on the bandwagon as well, including this one. It is the duty of the platform providers to guarantee that the devices they host are secure since they are hosted on closed platforms. This article focuses on manufacturing and related enterprises. One industry after another is looking for methods to increase security as they link more and more equipment to the internet, whether it's in manufacturing, oil or gas, refining, medicines or food and beverage. Device manufacturers and plant operations managers are under constant pressure to protect their physical assets from cyberattacks. Data characteristics, IoT topologies, and issues in threat management and compliance are specific to each of these enterprises.” [9]

Mohit Saini et.al (2019) “People, smart gadgets, intelligent things, information, and data were all transformed by the Internet of Things (IoT). Increasing the number of gadgets that connect to the internet has made it more difficult to secure the data they communicate and the connections they originate. In recent years, we've witnessed a significant increase in the number of IoT devices in both households and factories. Using the Alexa Voice Service, we've seen a whole ecosystem spring up around Amazon's Echo devices in the first case. This isn't the only company that has jumped on the bandwagon. The responsibility for safeguarding these devices is on the platform providers, as they are autonomous and closed. Cyber security in the manufacturing and allied sectors is the focus of this article. It's becoming more difficult to find the correct level of security for industries such as manufacturing and oil & gas; refining; pharmaceuticals; food and beverage; water treatment; and many more, as more and more equipment and devices are brought online. There is a continual strain on device makers and

plant operations managers to secure their physical assets from cyber-attacks. In addition, the nature of the data, the topologies of IoT devices, and the difficulties of threat management and maintaining compliance are all different for each of these businesses."

KAZI MASUMSADIQUE (2018) " In the "Internet of Things" paradigm, "things" are defined as "things" that have been merged with electronics, software, sensors, and a connection. Servers, centralised systems, and/or other linked devices may exchange data with these "things" using a number of communication infrastructures. Using an internet connection, sensors, nodes, and collectors send their data to a cloud server. "Internet of Things" IoT devices are used by consumers, healthcare providers, companies, and governments. An estimated 31 billion "Internet of Things" IoT devices are expected to be in operation by the year 2020 throughout the world. Vulnerabilities related to the "Internet of Things" IoT are on the rise as the number of devices rises. According to the results and analyses, the widespread use of "Internet of Things" IoT and the inclusion of new technologies is bringing with it new security risks. Future research on IoT security issues and open questions may be found in this article. [10]

THE EFFECT OF IoT FEATURES ON SECURITY AND PRIVACY

1) Description: More and increasingly IoT devices mean more complicated device-to-device interactions that need less and less human intervention. When it comes to the "Internet of Things" (IoT), gadgets no longer interact with each other in the same way as conventional computers or smart phones. IFTTT (if this, then that) is a popular service in numerous IoT application situations, and many of them may be controlled by other multiple devices' actions or environmental circumstances. Suppose the thermometer detects a rise in the inside temperature while the threshold and smart plug recognize that the air conditioner has been switched off. In this situation, the windows would automatically open. Industrial and agricultural devices are more likely than other types of devices to have similar incidents. In this context, we refer to this link of implicit dependency between devices as an IoT feature referred to as "Interdependence" in this context.

2) Threats: The attackers may not be able to get access to the target device or system, but they may be able to affect the behavior of other devices or the surrounding environment to accomplish their goals. When exploited in an unintended manner, this functionality might make it easier for attackers to target devices and evade their initial defensive mechanisms. There is no need for hackers to get into the automated window control or the thermometer to achieve their purpose in the previous paragraph. It's possible that instead of shutting off the air conditioning, he could hack the smart plug, which would enable him to open the windows and break through the building's perimeter.

3) Challenges: There is a lack of knowledge of how interdependence impacts the security of the "Internet of Things," which is a growing concern (IoT). The researchers are usually the

ones who keep an eye on the lone device. Creating a defined defensive perimeter for IoT devices, as well as using static access control techniques and privilege management, is challenging due to the interrelated behaviour of IoT devices. “Today, many Internet of Things IoT devices are being handled by cloud-based platforms programmes (for example, Smart Things, Samsung Smart Things, Apple HomeKit, Amazon Alexa, JD.com, and Ali), which have already gained popularity among smart home users. In order to prevent their behaviour from being affected by other devices or environmental factors, it is necessary to define a special set of fine- grained authorization rules for Internet of Things IoT devices.” There is a problem with over-privilege in the programmes that are now running on IOT platforms.

4) Solutions & Opportunities: Because of this, the Carnegie Mellon University team came up with a set of new security protocols to identify interdependent anomalies early on. However, as the number of devices grows, these restrictions will become increasingly difficult and unworkable. Earlier this year, Yunnan et al. introduced Context IoT, a novel context-based authorization framework for IoT platform applications, to address the issue of over privileged IoT platforms. Using this information, the user may decide whether or not to accept or refuse an IoT device activity depending on the context of the process or data flow, as well as the runtime data. An early detection of IoT device dependent abuse is possible with this way. Because even if hackers engage in malicious conduct under identical environmental circumstances to the norm, it is difficult to get the same level of contextual knowledge as is available from official data sources. It's an approach that relies on user decisions too much; if they choose the incorrect thing, the system will remember that they did and not bother them again. As a result of the dependency, more effective and practical solutions are urgently required.

METHODOLOGY

We used Elsevier, IEEE, Springer, and MDPI databases to gather data for our study. As a result, we were able to reduce the number of options to 37.
In order to achieve the problem's goals, this report must address the following AQs:

- What are IoT applications?
- How would you sum up the limits of the IoT?
- In what ways might IoT be improved?
- Which IoT application approaches are evaluated based on a variety of characteristics?
- What Threats and limits of IoT applications in the present and future are discussed?

Figure 1 depicts the publishing process for disseminating research findings. A respectable scientific publisher's papers about the research process are included in this category.

Figure 2 depicts the proportion of articles published by various publishers, which can be seen in the graph. The Elsevier has the largest proportion, at 36%, as can be shown in the figure.

IEEE with a 28% share, followed by other publishers with a 23% share, MDPI with an 8% share, and Springer with a 5% share.

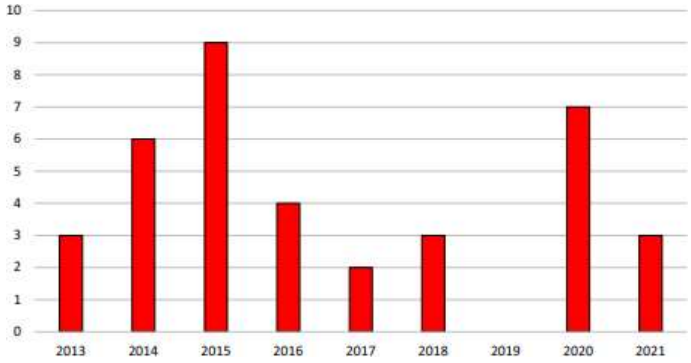

Fig. 1 "Distribution of research papers by the publisher"

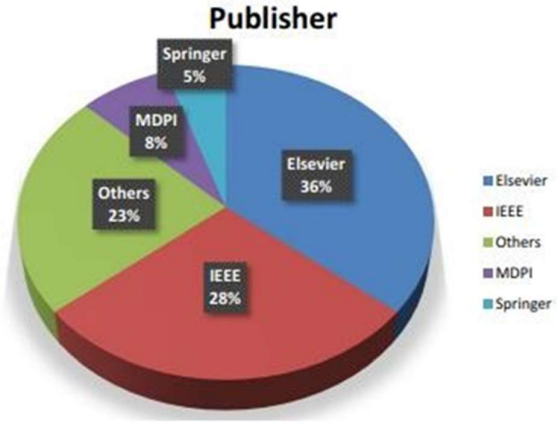

Fig. 2 "Percentage of published research papers by different publishers"

DATA ANALYSIS

The IoT data accessed and retrieved will also gather critical data that can be communicated from production and manufacturing industrial systems and employed in the enterprise's information system. Sensors and data terminals in manufacturing, storage, and databases, as well as on-premises or cloud-based application services, all provide real-time data streams. By reducing the chance of human mistake, smart devices in the manufacturing process will guarantee that decision support systems analyze current information in real time.

The main features of IOT applications are as follows:

- Information that has been disseminated worldwide Smart devices and networks will be able to make their own judgments and take charge of their surroundings instead of being reliant on a centralised control system. Automated equipment in the manufacturing process is able to operate at a consistent frequency and make energy-saving decisions. They may communicate with other machines in the same factory or cloud system via an

indirect way of communication. A cloud-based manufacturing process may be changed in real time by a smart manufacturing equipment.

- Streamlined communication channels It is essential for IOT applications to have a fast connectivity infrastructure to support real-time output. This necessitates the development of new communication protocols based on fibre infrastructure, in particular for in-plant communication. Using OPC UA (OPC Unified Architecture), the OPC Foundation developed protocols to link machines (M2M Communication).

- Systems and standards that are free to use IoT application developers will be able to create cost-effective and flexible solutions without being reliant on a single supplier because to the interoperability and programming language compatibility of production devices created by different firms.

- Production and data transmission in real time these systems are able to respond quickly to issues in production, such as changes in demand and the availability of raw materials. Real-time monitoring of production data, on the other hand, will give a significant competitive and financial advantage.

- IoT research The main properties of IoT enhance manufacturing quality, costs, energy efficiency, performance, and dependability significantly:

1. Wireless communication batteries are used by sensor devices to provide the energy they need. They are able to communicate with their network.

2. These systems may be employed in huge numbers due to their low cost. Sensor device data may be stored and used for many purposes, such as configuring, monitoring, or analyzing large data. It is used in corporate decision-making processes for evaluation and analysis.

3. The proper individual receives the information thanks to data analysis.

4. In the event of a loss of output, corrective action is taken immediately and effectively by the relevant personnel.

From smart homes, industries, cities and agriculture to health and wellness applications, the "Internet of Things" IoT offers the potential for a broad variety of transformations. An extensive industrial area is covered by it.

Sensor networks connect with wireless networks in a restricted frequency band in the Internet of Things. The importance of dynamic cognitive-communication techniques is growing. Some of the IoT's downsides include the following: As the number of connected devices rises and

the amount of information transmitted between devices increases, hackers become increasingly capable of stealing private information. IoT devices might grow into millions in the future, and handling data from all of these

devices is going to be a challenge. If there is a problem with the system, it is quite likely that all associated devices would be affected. There is no uniform standard for IoT, therefore devices from various manufacturers cannot communicate with each other.

There are a broad variety of applications for the "Internet of Things" IoTthat may enhance our daily lives and enterprises while also reducing expenses and energy usage. The IoT's benefits include:

- Observe the main workings of a company
- Time and money saved
- To enhance client satisfaction
- Making more intelligent business choices
- Intensifying motion
- To increase one's earnings
- Incorporating and energising enterprise models

Product quality, efficiency, and performance are all areas where it might have a big influence. However, in order to fully reap the benefits of the Internet of Things, both technical and political challenges must be overcome.

The following is a list of some of the many unresolved problems in the Internet of Things:

- extraction of information from data and its subsequent transformation current issues in data mining and intelligent computing In the future, IoT's billions of connected devices and the massive amounts of data they generate will be even more important.

- Identifying and managing one's identity The “Internet of Things” IoT and smart gadgets will connect billions of sensors. As a result, each item must be given a unique name or identifier. It's also necessary to establish a management strategy to deal with this problem.

- Standards and conformity in the “Internet of Things” Other smart gadgets are produced by several firms. As a consequence, gadgets from different manufacturers cannot communicate with one other. Problems with compliance and the creation of uniform standards are two of the most pressing concerns that need to be addressed.

Technology, Architecture, and Security; and Applications are the four main types of IoT issues.

IoT applications are characterized by their ability to move around. There are a number of issues we confront because of the application platform's ability to move around, such as dynamic IP allocation and network overhead. Because of this, IoT applications may experience intermittent service interruptions when using the affected gateway.

An application may be used on a wide range of platforms. Manufacturing and connection protocols differed amongst these devices, but they were all serviced by a same server.

Table 2 Comparison of IoT application assessment factors

Research	Mobility	Complexity	Error-ness	Cost	Security	Real-time-ness	Availability
Cho et al.	×	✓	×	✓	×	×	×
Felisberto et al.	✓	✓	✓	✓	×	×	×
Fang et al.	×	✓	×	✓	✓	✓	✓
Gutierrez et al.	×	×	×	✓	×	×	×
Ashokkumar et al.	✓	✓	✓	✓	✓	✓	✓
Abashidze et al.	×	×	✓	×	✓	×	×
Jacobsson et al. [	✓	✓	✓	✓	✓	✓	✓
Hossain et al.	×	✓	✓	✓	✓	✓	✓
Ding et al.	×	×	×	✓	✓	✓	×
Wei et al.	✓	×	×	✓	✓	✓	✓
Chaudhry et al. [	✓	×	✓	✓	×	✓	✓
Jia	×	×	×	✓	×	✓	✓
Mabrouki et al.	×	×	✓	×	×	✓	×
Mircea et al.	✓	×	✓	×	✓	×	×

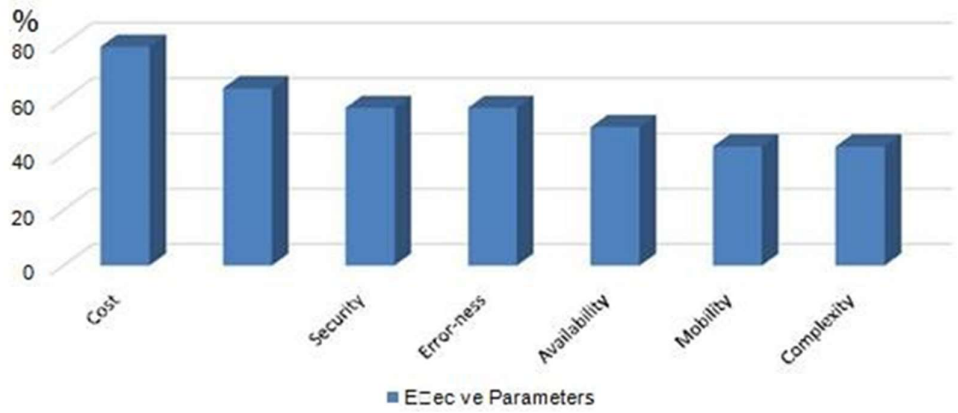

Fig. 6 “The assessment of the evaluation factors for IoT applications”

Application in other areas as a result, addressing the problem of scalability is essential. To get around this problem, it's going to take a lot of hard work and money to integrate protocols and standards.

Many “Internet of Things” IoT apps cater to devices that run only on batteries. However, if the battery fails or dies, or if the mobile power source is unavailable at a key moment, the service may be disrupted. To provide uninterrupted service, it is critical to ensure that IoT components have sufficient power. As a result, battery lifespan studies should be done. Implementing hardware redundancy and offering backup batteries, or even harvesting energy from renewable sources like solar power, might be considered in the future.

Services in IoT applications are still under investigation. As a result, service deterioration due to a poor network, low-speed Internet and massive data quantities must be addressed. Although cloud platforms offer a good solution to these issues, they are always evolving and may be improved upon.

In the “Internet of Things,” data security and confidentiality are crucial because of the many issues posed by the technology's lossy or restricted identification.

A new generation of mobile communication technologies, 5G, was created to address the shortcomings of 4G and increase its performance. Its high connection density and low latency make it ideal for a broad variety of applications in both technology and human life. All smart areas, such as healthcare and transportation (including autonomous cars and virtual reality), will benefit from IoT communication in a 5G- enabled world.

CONCLUSION

An initial screening study was undertaken to determine which sectors of the "Internet of Things" may benefit most from IoT implementations such as medical diagnostics and home automation as well as agricultural and urban planning. Sensor technologies,

in particular as they have grown more affordable and simpler, have made it vital for us to maintain constant contact with the items we use on a daily basis.

The "Internet of Things" (IoT), computing, and communication are on the verge of a technological revolution propelled by rapid advances in fields like wireless sensors and nanotechnology. Numerous businesses may benefit from this technology, from retail to healthcare to manufacturing. The term "Internet of Things" refers to a collection of devices that interact with the environment, communicate with one another, and may be managed over the Internet (IoT). By 2020, "Internet of Things" IoT is predicted to outpace both PCs and the Internet in terms of global market share.

REFERENCE

1. Amir Masoud Rahmani (2022) ," "Internet of Things" Applications: Opportunities and Threats," Wireless Personal Communications volume 122, pages451–476

2. N. Mishra and S. Pandya, ""Internet of Things" Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

3. Ali, Rao & Muneer, Amgad & Panneer Selvam, Dhanapal Durai Dominic & Mohd Taib, Shakirah & Ghaleb, Ebrahim. (2021). Internet of Things IoTSecurity Challenges and Solutions: A Systematic Literature Review. 10.1007/978-981-16- 8059-5_9.

4. Mohit Kumar Saini, Rakesh Kumar Saini, 2019, Internet of Things IoTApplications and Security Challenges: A Review, International Journal of Engineering Research & Technology (IJERT) NCRIETS – 2019 (Volume 7 – Issue 12),

5. Kazi MasumSadique (2018)," Towards Security on Internet of Things: Applications and Challenges in Technology," Procedia Computer Science Volume 141, 2018, Pages 199-206

6. R. Vignesh and A. Samydurai ans1 Student, 2Associate Professor Security on "Internet of Things" IoTwith Challenges and Countermeasures in 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939.

7. Shaukat Dar, Kamran & Mahboob Alam, Talha & Hameed, Ibrahim & Khan, Wasim & Abbas, Nadir & Luo, Suhuai. (2021). A Review on Security Challenges in Internet of Things (IoT). 10.23919/ICAC50006.2021.9594183.

8. J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1- 2, 2014.

9. Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter- System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.

10. Noshina Tariq et.al (2021) “Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis”, Procedia Computer Science, Volume 191, Pages 425-430

11. B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604- 608, 2012.

12. M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5,86-97, 2012.

13. R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172, 2014.

14. Mirza Abdur Razzaq and Muhammad Ali Qureshi “Security Issues in the “Internet of Things” (IoT): A Comprehensive Study” by (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.

15. M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.