ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1837

Recent Developments in IoT Security and Privacy: A Review of Best Practices with Challenges and Emerging Solutions

Dr. Sunita Dixit[1]; Dr. Dinesh Yadav[2]

[1]Professor; [2]Associate Professor
[1,2]Department of Computer Science & Engineering,
St. Andrews Institute of Technology & Management, Gurugram, Haryana, India

Publication Date: 2025/04/02

Abstract: The Internet of Things has changed many fields by making it easy for smart devices to talk to each other. On the other hand, this change has led to major security and privacy problems, such as malware attacks, unauthorized access, data leaks, and weak authentication systems. IoT gadgets are easy targets for hackers because they often don't have a lot of processing power. Additionally, the massive data generated raises privacy concerns regarding unauthorized surveillance and data misuse. Traditional security measures are insufficient for IoT ecosystems, necessitating innovative solutions. Emerging approaches include blockchain for decentralized security, AI-driven anomaly detection, lightweight encryption techniques, and zero-trust architectures. Regulatory frameworks and technologies that protect privacy, such as federated learning and differential privacy, are also becoming more common. Even with these changes, it's still hard to find a good balance between privacy, security, and usability. It talks about the newest threats to privacy and security in the IoT as well as fresh methods to protect and strengthen the environment.

Keywords: *Component, Formatting, Style, Styling, Insert.*

How to Cite: Dr. Sunita Dixit; Dr. Dinesh Yadav. (2025). Recent Developments in IoT Security and Privacy: A Review of Best Practices with Challenges and Emerging Solutions. *International Journal of Innovative Science and Research Technology*, 10(3), 1888-1894. https://doi.org/10.38124/ijisrt/25mar1837.

I. INTRODUCTION

The 21st century is sometimes called the "age of wireless communication and interconnectedness," and computer networking technology has come a long way. The word "IoT" was his brilliant idea. Using the IoT, digital and real-world objects can connect and talk to each other. With wheels and sensors, intelligent IoT devices can sense their surroundings and work on their own. These devices can be very small and wearable or very big and industrial[1].

As more organizations use IoT, more IoT devices and apps will become available. Companies that manufacture gadgets that track and exchange data about an individual's behaviors and health are the makers of wearable technology. For instance, IoT software and devices are becoming available to healthcare professionals. A "smart house" IoT tool today includes a video doorbell, lights that talks to you, a smart coffee maker, and a smart door lock. Now that there are a lot of "smart city" apps and IoT devices available, you can do things like smart parking, smart street lighting, and smart trash management.

The safety of IoT devices has been one of the most talked-about themes among researchers. The IoT has a lot of good points, but its three biggest problems are sending data, collecting data, and the safety of that data. A lot of tracking apps are made to get data from IoT devices. To send and receive data, protocols have been made and changed. This lets Internet of Things (IoT) devices share info and connect to networks that are already set up. That being said, they don't follow these rules right. Because of this, the IoT is directly connected to a number of new and old security issues, such as authentication, data protection, and permissions. Attacks such as guessing passwords, repeat, Denning-Sacco, loss of service, and more can happen if you don't log in. There are, however, a lot of networks that make it hard to check IoT devices. Blockchain could make the IoT better, and protocols that run on IoT devices should take into account how little power, memory, and computer power they have. Concerns about IoT safety and security were talked about. This is done by finding common threats and ways to attack IoT devices, as well as showing weak spots that could allow a security breach. Along with fixes for devices that had been hacked, this document also had a number of security changes and ways to lower risks. New technologies like blockchain and software-defined networks (SDN) make IoT

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1837

networks safer. The best things about these two security systems are that they can be expanded and changed easily. Another part of the study looked at the problems and needs for safety in various IoT apps. Classic and modern security choices are the two main types.

Security for the IoT has been studied before. The main topic of this study's investigation into security and IoT research is how data security is used and what worries there are when it comes to network security [2]. Through the following objectives, this evaluation seeks to address the pressing challenges shown in Figure 1. and research questions (RQs):

This is the division of the remaining tasks. explains briefly about the context and goal of the study. has committed to:

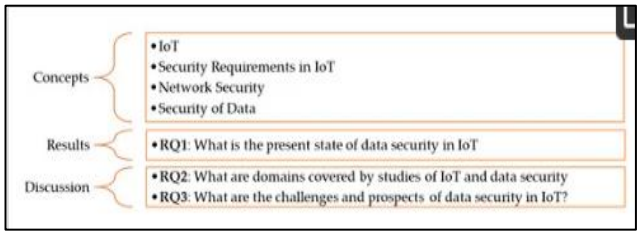

Fig 1: The Studys Objectives

II. OVERVIEW OF IoT

This internet of things (IoT) can be used in various methods to fulfil various purposes. Services involved in device modelling, device control, data publishing, data analysis, and device detection" are some of the different things that the IoT can do. Other technologies in the same field become less important as IoT grows because it could make it easy to learn and get around. We need to look at some of the ways that the IoT keeps changing the brain if we want this technology to last [2]. What each writer about IoT says is different. It's defined as "an interconnection of machines and devices through the internet [3], allowing the creation of data that can shed light on analytic performance and support new technologies." As stated, "the IoT is a collection of interconnected static and/or mobile objects, such as devices with communication, sensor, and actuator modules connected through the internet." Basically, the "IoT" is a group of real things that can talk to each other on their own.

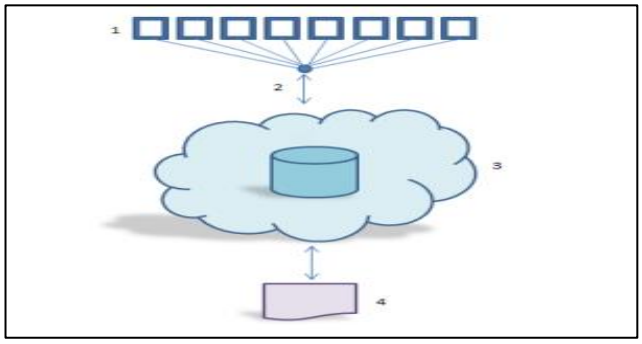

Fig 2: Simple Diagram of the Operation of IoT

Data must be sent from Element 1 to Element 3 through Network Element 2 by each block in Figure 2. Thus, Figure 2 displays a broad view of how the IoT is built. These blocks are connected by lines that go up and down. Part 3 is also known as "the cloud," and it cleans, stores, and processes the data so that Part 4 the end user or service hiring party can get the results.

A. Devices

One type of device is an IoT endpoint. This device records information while keeping an eye on a particular goal. Sensors are used to gather data on the important components, such as position and other multimedia-relevant information, in order to do this [3].

B. Network

"Nowadays, the internet has become available everywhere and has spread notably faster than any other technology," the author notes. "The network is the solution to the need of transporting knowledge over huge areas with little effort."

C. Security

One of the most important things about technology is that it is safe. The data that is gathered is private and important, so it is necessary for the progress of all technologies. The safety of this system is the same as that of any financial transaction.

D. Cloud

One more advantage of this technology is the cloud. The task involves storing, managing, and maintaining the security of the data blocks that are received from the devices.

E. IoT Security and Privacy Challenges

IoT has helped users a lot, but it has also caused some problems. The researchers and security experts who were named are mostly worried about privacy and hacking risks [4][5]. Because of these two things, both public and private groups are having a hard time. An increasing number of well-known cyberattacks have shown where IoT systems are weak.The interconnected networks of the IoT make it possible to reach the public and unreliable Internet, which makes this vulnerability possible. New security measures are needed to protect against this.

F. Security

IoT is not the same as regular computers and other electronics, so it is more likely to have security problems in several ways.

- A lot of IoT gadgets are being made to be used by a lot of people. This is very clear when you look at sensors.
- IoT setups usually include a group of appliances that are the same or very similar and have similar features.

The man-in-the-middle attack is one of the most common ways to hack into and damage the IoT. This happens when a third party takes over a communication route to look like one of the real network nodes involved in the exchange. The attacker doesn't even need to know the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1837

name of the supposed target in a man-in-the-middle attack to convince the bank server that the transaction is real[6].

G. Privacy

The usefulness of the IoT will be judged by how well it fits people's personal tastes. People might not want to use the IoT because they are worried about bad things happening and their safety. Being able to connect to the Internet from anywhere is also important for understanding this problem [7][8]. Because there won't be a special way to do it, it will be easier to get personal information from anywhere in the world.

H. Interoperability

It is well known that a fragmented world with proprietary IoT technology implementation makes things less useful for users.

- **Occasional update:** Every three months, IoT makers usually put out security updates.
- **Occasional update:** Security updates are usually released by IoT manufacturers every three months.
- **Embedded passwords:** IoT devices store passwords in-built, which lets support staff install updates or fix problems with the operating system from afar.

III. EMERGING SOLUTIONS FOR IOT SECURITY AND PRIVACY

A. IoMT Privacy and Security Solutions

Recently, many privacy and security tools have been made to stop people from misusing IoMT [9]. Moreover, cyber threats are increasingly aimed at IoT devices and apps [10], including IoMT, which emphasizes the need to put in place a number of important steps to deal with these problems [11].

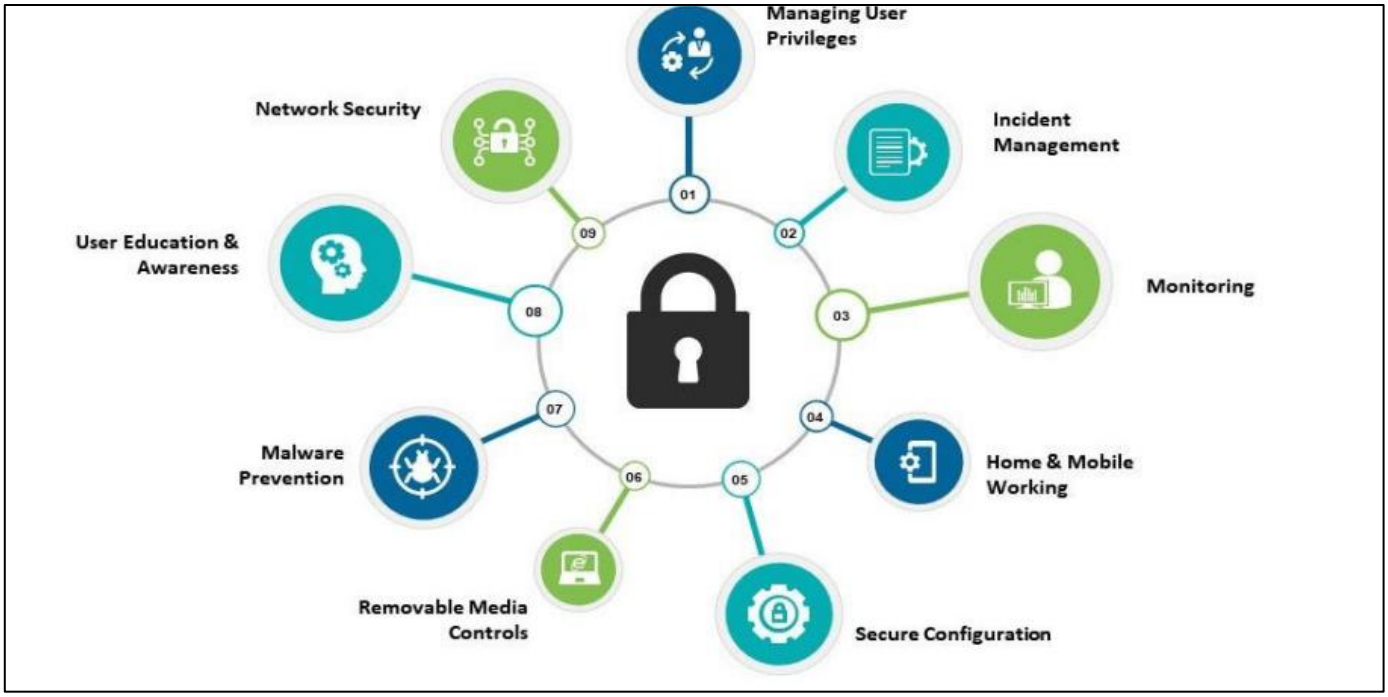

Fig 3: Security Areas in IoMT

Figure 3 shows a rough sketch of the IoMT's security areas. Figure 3 shows that IoMT has a number of security issues, such as when it comes to protecting malware or tracking patients.

IoMT is still very new, and there are security risks because of low standards, systems that aren't well managed, and users who don't know what they're doing. Hackers and enemies can quickly take over IoMT devices that aren't properly protected by using malware to hold the devices hostage and demand a fee. Wearable tech, smart houses, and apps are all hurt by the way IoMT devices are managed. More research needs to be done in this area before IoMT devices can be made safer against this type of attack.

Hackers can get into IoMT devices because companies put out new products quickly and don't update software often enough to stay competitive [12]. During an upgrade, the user's IoMT gadget and the cloud might not be able to talk to each other. Hackers can get into IoMT devices that aren't encrypted if they can talk to them without encryption. It is important for businesses to quickly limit access and ports in case the cloud link goes down. To keep security up to date, IoMT devices must also be updated [13].

B. Major Security Issues in iot

Modern Internet started with the Internet for Computers (IoT), which let machines talk to each other (M2M). Cheaper prices and more gadget support are needed for the IoT to be widely used [14]. This goal of increasing IoT use needs to be met first by fixing a few technology and security issues.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1837

C. Identification

It is important to figure out which device is which the original or a bad node. There needs to be a manufacturer's reference.

D. Authentication

One of the main problems with the IoT is that there are so many gadgets that want to connect. It's hard to authenticate every single gadget. Because they are fast and use little energy, private key encryption primitives have been used in a lot of security solutions.

E. Data Management

One of the hardest things to do is to find and fix all the billions of gadgets. Figure 4 shows that by 2020, there will be more than 50 billion smart devices that can connect to the internet.

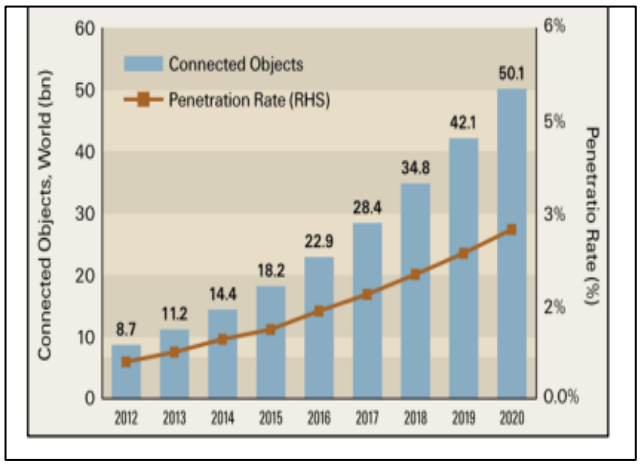

Fig 4: By 2020, 50 Billion Things will be Connected to the Internet

F. Heterogeneity

In terms of security and privacy, the device itself is by far the most hazardous kind. For the IoT to improve and become more dependable, issues must be appropriately resolved. monitoring hundreds of distinct device kinds, each with unique security requirements and concerns.

G. IoT Applications

IoT can provide a lot of different services, but only a few of them are commonly used. A lot of programs make people's lives better. IoT uses can be broken down into the main groups shown in Figure 5 These include retail, consumer, environmental, auto, medical, military, and industrial. IoT is used in health care, services and transportation, personal and social life, and the smart environment [13] (smart office, smart home).

H. Medical Applications:

The medical IoT market is growing quickly. It has many uses, such as remote tracking systems, smart sensors, and integrating medical items. IoT in healthcare can also help patients get better appointments and be happier by letting them talk to their doctors for longer amounts of time.

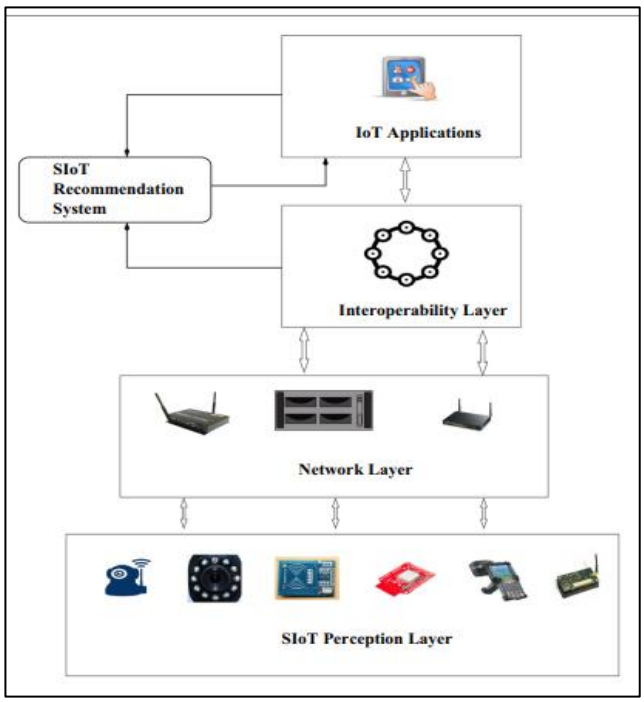

Fig 5: SIoT Architecture

I. Military Applications

These days, military actions are carried out in a situation that is complicated, multifaceted, very different, and sometimes difficult, with allies and enemies that aren't expected. More and more, military officers don't have time to get a clear picture of the situation before they have to decide on a strategy.

Useful Apps for Business If you use the IoT in business, you may hear the term "industrial internet of things" (IIoT). Companies can make their equipment work better and speed up their processes by collecting, managing, and analyzing sensor data through the IIoT. Many things can be used with it, like production control, smart meters, machine-to-machine contact, and motion control.

J. Environmental Applications

Environment monitoring can use IoT for things like managing waste and water, tracking animals, keeping an eye on and predicting the weather, protecting the environment and endangered species, gardening for profit, and more. Objects in these applications can find and measure all kinds of changes in the surroundings.

IV. LITERATURE REVIEW

Hassan and Awad (2018).looks at the pros and cons of deploying IoT in homes, towns, and regions from the point of view of security and privacy. Because of the IoT, life will continue to change, especially in cities. Putting the IoT paradigm into action will be hard in cities, though, where links are often not safe. As long as people are seen as "things" in the IoT paradigm, IoT gadgets could invade their privacy and take away some of their humanity. Because of worries about IoT, privacy groups for IoT and national and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1837

foreign privacy laws need to protect people's right to privacy and meet the privacy needs of cities' institutions [15].

Singh and Kumar (2020).The point of this paper is to look closely at some privacy and security issues that come up with the IoT. The main security and privacy problems are explained, along with possible solutions that have been taken from past research projects. These problems are shown by pointing out the biggest problems in the research field and some of the current answers, along with what they could mean for the future [16].

Zainuddin et al (2021) will look at what has already been written about privacy risks in the IoT, privacy issues in different IoT applications, and give a general outline of the study. A huge amount of data comes from many places, like governments, manufacturing companies, smart cities, and healthcare centres, and is processed by different IoT applications. Customers of these smart products are mostly worried about two things security and privacy. This is because IoT is used by so many people and opens up so many possibilities[17].

Sadkhan and Salam (2021) provide examples to look at privacy and security threats from the point of view of the IoT's layers. Additionally, a more complete example of one type of IOT smart home IOT system will be used to talk about the methods used to solve these problems and their flaws. When we get past these limitations, we'll talk about some of the unsolved security issues and some of the security problems that come up with the Codomain. Using a strategy, we have also suggested more work that should be done [18].

Alwarafy et al (2021) talks in great depth about the privacy and safety problems that come up with IoT that uses EC. To be more specific, we will first talk about EC-assisted IoT in general terms, such as what it is, how it works, and the pros and cons of it. After that, we talk about what privacy and security mean for IoT with EC. Then, we talk about the main risks of EC-assisted IoT in more depth, offer possible solutions and defenses, and name important research projects. Here are some of the security and privacy issues we've talked about so far, broken down into even more groups based on their jobs, goals, and the security services they offer. On the last page, there is a list of open questions and possible study paths for the secure EC-assisted IoT paradigm [19].

Table 1: Summarizes Key Objectives, Methods, Findings, Advantages, and Future Research Directions Related to Security and Privacy Issues in IoT Deployment Across Various Domains

Ref	Objective	Method	Key Finding	Advantages	Limitations & Future Work
[15]	Look into the privacy and safety problems that come up when IoT is used in cities	Review of privacy laws and IoT privacy groups	IoT devices can invade privacy and raise security concerns, requiring legal protection	Legal frameworks help protect privacy rights	Challenges in enforcing privacy laws across different regions
[16]	Find the biggest problem areas with IoT security and privacy and suggest ways to fix them	Analysis of past research projects	Concerns about IoT security and privacy are valid, but there are several ways to handle them.	Solutions from previous research provide insights into privacy protection	Some issues remain unresolved, requiring further research
[17]	Analyze privacy risks in different IoT applications	Literature review on privacy risks and IoT applications	Security and privacy are primary concerns due to widespread IoT usage	IoT enables smart cities and healthcare advancements	Privacy risks increase as data is collected from multiple sources
[18]	Investigate security and privacy attacks across IoT layers with a focus on smart homes	Scenario-based analysis	IoT layers have vulnerabilities; smart home IoT faces major security risks	Layered analysis provides a structured approach to addressing security threats	Some security challenges remain unresolved, requiring future frameworks
[19]	EC-assisted IoT makes things safer and more private.	An in-depth look at IoT with EC help, security risks, and possible solutions	Edge computing (EC) improves IoT efficiency but introduces security risks	EC offers benefits like reduced latency and better resource utilization	Security threats need further classification and additional defensive measures

V. FUTURE DIRECTIONS AND OPEN RESEARCH AREAS IN IOT

The Internet of Things (IoT) has helped businesses and smart places, but things have changed recently. The Internet of Things (IoT) lets separate devices, like computers, tablets, and smartphones, talk to each other. They send data about their surroundings to the people who use them. For local services like gathering data [20], the IoT idea depends on things being able to talk to each other. Connecting devices to servers, such as cloud servers, edge servers, or data hubs, is needed for high-level services like network tracking and data management. The lifecycle of data now includes AI and ML methods at all stages, from when IoT devices create or collect

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1837

data to when end users use it. These changes are needed to meet the new service standards and high-quality service needs of current IoT applications. A new type of IoT networking called Intelligent IoT (IIoT) combines smart solutions with machine learning and artificial intelligence. This paradigm has changed how IoT apps work in areas like smart industry, smart transportation, and smart healthcare. IIoT specifically offers many ways to improve devices (for example, using AI models on nearby IoT devices to make them better) and provide services (for example, AI-assisted data management and smart data transmission). AI is used in IoT networks to improve the user experience and make network processes more cost-effective. Patients can now use smart features like automatic disease detection in IoT systems aimed at healthcare and traffic forecasting in smart IoT networks for vehicles. AI can also be used in IoT systems to help businesses in many ways. These include precise cost reductions by getting rid of human error, predictive maintenance to cut costs and keep businesses running, better customer service to make customers happier, more scalability to handle large IoT ecosystems, and higher operational efficiency through smart automation and pattern recognition. Commercial AI uses in IoT are now popular in a number of fields. In industry, for example, robots with sensors and artificial intelligence make the work more efficient. AI is used by self-driving cars to plan their moves and make the roads better. AI-powered analytics and smart devices like security cams and smart shopping carts make the retail industry better at serving customers and running its business. Artificial intelligence (AI) is used in healthcare wearable tech to track and report health data, which encourages early treatment. Industry and services that are smart. In particular, IIoT opens up a lot of opportunities for service delivery, such as AI-assisted data management and clever data transmission, as well as device improvement, such as putting AI models on local IoT devices to make them smarter. AI is used in IoT networks to improve the user experience and make network processes more cost-effective. Patients can now use smart features like automatic disease detection in IoT systems aimed at healthcare and traffic forecasting in smart IoT networks for vehicles. AI can also be used in IoT systems to help businesses in many ways. Among these are lower precision costs because people won't make mistakes, cheaper and more reliable maintenance to keep businesses running, better customer service to make customers happier, the ability to handle large IoT ecosystems, and higher operational efficiency through smart automation and pattern recognition.

VI. CONCLUSION AND FUTURE WORK

Internet of Things (IoT) makes "smart cities" possible. Big issues like pollution, lack of resources, and crowds are being worked on by these cities. Very detailed study of the Internet of Things (IoT) technologies, uses, and building blocks that allow smart towns to exist. When it comes to smart trash management, IoT lets us gather, look at, and make decisions in real time. Other areas are smart energy management. By making public services better, lowering their negative effects on the environment, and making the best use of resources, these examples show how IoT-driven solutions can greatly raise the standard of living in cities.

Future research should focus on making IoT systems more energy efficient, making communication methods that work reliably, and keeping IoT systems safe and private. Additionally, progress in bitcoin, AI, and 5G and 6G technology could lead to smart city solutions that are stronger and more adaptable. IoT can continue to change how people live in cities by addressing these problems. This will make cities safer, smarter, and more environmentally friendly for future generations. Also look into what the pros and cons of the IoT are. Although there are many benefits, risks can be used to put end users in danger by letting attackers into systems, letting unwanted people see private information, and putting people's safety at risk[9]. have to make sure that IoT-enabled goods ships have the right security features that affect how they work, how easy they are to use, and how well they work with other systems. Also want to build a dynamic security system with the help of researchers that will cut down on, if not get rid of, security and privacy threats. Additionally, believe that this system will be intelligent enough to adjust to new forms of communication and various app deployment methods.

There are a lot of people who use the IoT, so businesses should put system security first. A lot of people would be affected by a hack or system failure caused by any weakness.Hackers can't get into IoT gadgets that are physically connected if they have smart IoT security. The things that IoT security teams often think about are inventory, operations, variety, management, data flow, attacks, and other things. This research is mostly about data security situations, uses, and problems that have to do with network security. It also looks at security and IoT research. Using the terms that were given earlier, 564 matches were found. 34 pieces were thrown out because they were too similar. As a result, 530 stories were taken out of the total. Each of these parts is looked at and put in order based on the rules that say what should be included and what shouldn't. The analysis looked at 25 studies that were released between 2012 and 2022 and met the criteria. Research shows that the IoT business has been responding for years by putting out IoT security technologies that keep devices and systems safe from threats and unauthorized access. Scientists and experts from many countries and fields are now interested in IoT network security.

The IoT often gives app makers the tools they need to collect, manage, and protect devices and data. People's lives are better and more comfortable when IoT devices talk to each other and work together. IoT makes it possible to watch things in real-time, automate inventory, and keep track of information and conditions. Because so much data moves between devices on the network, there needs to be a security system to protect data integrity, privacy, authorization, and identification. A lot of research has been done on how to improve proof by using different methods on different devices, even wireless ones.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1837

REFERENCES

[1]. V. Pillai, "System And Method For Intelligent Detection And Notification Of Anomalies In Financial And Insurance Data Using Machine Learning," 202421099024 A, 2025.

[2]. H. Taherdoost, "Security and Internet of Things: Benefits, Challenges, and Future Perspectives," *Electronics*, vol. 12, no. 8, 2023, doi: 10.3390/electronics12081901.

[3]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2015.2444095.

[4]. Z. Ali *et al.*, "A Generic Internet of Things (IoT) Middleware for Smart City Applications," *Sustainability*, vol. 15, no. 1, 2023, doi: 10.3390/su15010743.

[5]. M. Aldwairi and L. Tawalbeh, "Security techniques for intelligent spam sensing and anomaly detection in online social platforms," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, p. 275, 2020.

[6]. V. Pillai, "Anomaly Detection Device for Financial and Insurance Data," 6414579, 2025.

[7]. Srinivas Murri, "Data Security Environments Challenges and Solutions in Big Data," vol. 12, no. 6, pp. 565–574, 2022.

[8]. Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures," *IEEE Wirel. Commun.*, vol. 25, no. 6, pp. 53–59, 2018.

[9]. F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective," *Sustainability*, vol. 15, no. 4, 2023, doi: 10.3390/su15043317.

[10]. L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on Deep Learning approaches for IoT security," *Comput. Sci. Rev.*, vol. 40, p. 100389, 2021.

[11]. M. Gheisari *et al.*, "A survey on clustering algorithms in wireless sensor networks: challenges, research, and trends," in *2020 International Computer Symposium (ICS)*, 2020, pp. 294–299.

[12]. K. A. Raza, A. Asheralieva, M. M. Karim, K. Sharif, M. Gheisari, and S. Khan, "A novel forwarding and caching scheme for information-centric software-defined networks," in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, 2021, pp. 1–8.

[13]. R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," *Internet of Things*, vol. 14, p. 100365, 2021.

[14]. A. K. Manjulata, "Survey on lightweight primitives and protocols for RFID in wireless sensor networks," *Int. J. Commun. Networks Inf. Secur.*, vol. 6, no. 1, pp. 29–43, 2014, doi: 10.17762/ijcnis.v6i1.572.

[15]. A. M. Hassan and A. I. Awad, "Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges," *IEEE Access*, vol. 6, pp. 36428–36440, 2018, doi: 10.1109/ACCESS.2018.2838339.

[16]. S. Singh and D. Kumar, "Perceptions of Security and Privacy in Internet of Things," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 810–813. doi: 10.1109/ICICT48043.2020.9112462.

[17]. N. Zainuddin, M. Daud, S. Ahmad, M. Maslizan, and S. A. L. Abdullah, "A Study on Privacy Issues in Internet of Things (IoT)," in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, 2021, pp. 96–100. doi: 10.1109/CSP51677.2021.9357592.

[18]. S. B. Sadkhan and Z. Salam, "Security and Privacy in Internet of Things- Status, Challenges," in *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)*, 2021, pp. 308–312. doi: 10.1109/IICETA51758.2021.9717785.

[19]. A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, 2021, doi: 10.1109/JIOT.2020.3015432.

[20]. O. Aouedi *et al.*, "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," *IEEE Commun. Surv. Tutorials*, p. 1, 2024, doi: 10.1109/COMST.2024.3430368.