Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777818

# FUTURE RESEARCH ON INTERNET OF THINGS (IOT) AND IT'S APPLICATIONS

**Brij Bhushan Sharma**
Yogananda School of AI Computers and Data Sciences, Shoolini University of Biotechnology and Management Sciences, Solan, Himachal Pradesh.
Email: brijbhushan@shooliniuniversity.com

**A. Manimaran**
Department of Mathematics, Kongu Engineering College (Autonomous), Perundurai, Erode 638060, Tamil Nadu.
Email: manimarankongu@gmail.com

**Meerjumla Govind Raj**
Department of Electronics and Communication Engineering, Malla Reddy Engineering College (Autonomous), Maisamaguda, Dhulapally, Telangana.
Email: mgovindrajassitantprofessor@gmail.com

**Tiny Tanushree Gohain**
Department of Management, Brainware University, Kolkata, West Bengal.
Email: ttinystar@gmail.com

**A. Clement King**
Mount Carmel College (Autonomous), Bengaluru, Karnataka.
Email: clementking@mccblr.edu.in

**S. Rani**
Department of Information Technology (BCA/IT), Vels Institute of Science, Technology & Advanced Studies ((VISTAS), Chennai, Tamil Nadu.
Email: srani.scs@velsuniv.ac.in

**Abstract**

People, smart gadgets, intelligent objects, information, and data all form part of a worldwide network that has been fundamentally altered by the advent of the Internet of Things (IoT). It's no secret that the security of sent data and initiated communications is getting increasingly difficult to ensure as the number of connected devices grows. The proliferation of IoT devices throughout time may be broken down into two main categories: the household and the workplace. In the former case, an entire ecosystem has grown up around the Alexa Voice Service and Amazon's Echo devices. Technology giants like Google, Microsoft, and Apple have all joined the trend. Due to the restricted nature of these platforms, device security must be handled by the platform providers. In this study, we focus on the importance of manufacturing-related cyber security. As more and more machines and gadgets are brought online, industries including manufacturing, oil and gas refining, pharmaceuticals, food and

beverage processing, water purification, and many more are always trying to improve their security. Manufacturers of electronic devices and plant managers are under constant pressure to safeguard their facilities from cyberattacks. Furthermore, the complexity of threat management and compliance varies greatly between businesses due to differences in the types of data collected, the organizational structures of IoT devices, and other factors.
**Keywords:** Internet of Things, Cyber-attack, Security threats.

**Introduction**

The Internet of Things (IoT) has emerged as the fastest-growing technology in recent years, having a profound effect on both personal and professional spheres thanks to its quick expansion and diverse service offerings. The prevalence of IoT services coincides with the fast spread of IoT devices. Threats and assaults against Internet of Things (IoT) devices and services have increased in proportion to their popularity.

The concept of the Internet of Things (IoT) has the potential to significantly transform how we interact with electronic devices. Once considered science fiction, the idea of a future in which every electronic gadget is connected to a single network is becoming a reality. However, IoT is not only becoming a reality, but also a global phenomenon. The market for IoT devices has expanded significantly. IoT gadgets are starting to make their way into our (smart) homes, where they are predicted to have the greatest impact on our daily lives. The majority of smart home gadgets will be completely innocuous kitchen tools like toasters and kettles. A hacker might potentially ruin your morning without much success even if they manage to compromise these devices. Since IoT is still in its infancy, the market is now concentrating on its vertical divisions. However, Internet of Things cannot be viewed as a singular entity, platform, or technology. More attention must be paid to interfaces, platforms, mobile applications, and common/dominant standards if the rapid development anticipated from IoT prospects is to be realized. [1].

The Internet of Things (IoT) is already automating several aspects of the traditional education system; smart classrooms encourage student engagement and learning, while automated attendance and tracking systems have the potential to make schools safer. The advent of Internet-enabled remote classrooms will be a watershed moment for developing nations, allowing for widespread educational access in locations where building a conventional school infrastructure is prohibitively expensive or impossible. Results from Internet-connected factories and factories are differentiated through automated process controls, making them safer and more efficient. Advanced sensors, networked with high-powered microcomputers, are progressively providing plant and energy optimization, health and safety control, and security management. Many banking and investment services are already offered online. Innovations, such as smart wearable and smart monitoring devices, that help clients keep better track of money and investments could further boost the growth of the financial sector as digital infrastructure and the next generation of IoT enabled goods improve exponentially. While IoT-enabled devices may increase a telecommunications company's average revenue per user (ARPU), there are significant risks and challenges that must be addressed, including privacy and infrastructure security. Even if the potentials of these new technologies are staggering, they also show significant Internet of Things cybersecurity risks. The quantity and sophistication of assaults against IoT devices have skyrocketed in recent years. Cybercriminals now have a far

larger attack surface to target due to the increased interconnectedness of people, devices, and institutions in today's digital world. The organization's risk "landscape" is merely a small portion of a potentially contradictory and opaque universe of current and potential dangers, many of which originate from unanticipated quarters and can quickly escalate. Several issues with IoT security were covered in this study. This paper's primary contribution is a review of the present state of problems with IoT security [2-3].

**Internet of Things (Iot)**

The internet of things (IoT) is a network that connects various electronic gadgets, mechanical and digital machines, objects, animals, and even humans, all of which are assigned a unique identifier (UID) and are capable of exchanging data with one another automatically, without any need for human intervention. A person with an implanted heart monitor, a farm animal with a biochip transponder, a car with built-in sensors to alert the driver when tire pressure is low, or any other natural or man-made object that can be given an IP address and transfer data over a network are all examples of "things" in the internet of things [4]. More and more businesses across a wide range of sectors are adopting IoT strategies in order to boost productivity, gain a deeper understanding of their customers so they can provide better service, make more informed decisions, and grow their enterprise's value [5]. The term "internet of things" (IoT) refers to the idea that commonplace physical objects may be linked to the internet and could communicate their unique identifiers to other devices across the network. Although radio frequency identification (RFID) is commonly thought of when this phrase is spoken, other sensor technologies, wireless technologies, and even QR codes might be included.

**Characteristics of Internet of Things (Iot)**

Some most popular characteristics of Internet of things are:

a. Intelligence
b. Connectivity
c. Dynamic Nature
d. Enormous scale
e. Sensing
f. Heterogeneity
g. Security
h. Intelligence

The intelligence of the Internet of Things originates from the interplay of algorithms, computation, software, and hardware. With the help of ambient intelligence, IoT devices are better able to adapt to their surroundings and do the duties assigned to them. Popular as smart technologies may be, intelligence in IoT is only concerned as a means of interaction between devices; interaction between users and devices is accomplished through the use of conventional input methods and a graphical user interface [6]. Algorithms and compute (i.e. software and hardware) together generate the "intelligent spark" that gives a product its smart feel. Compare the Nest intelligent thermostat to the fitness tracker Misfit Shine. The Shine feature splits processing duties between a user's mobile device and the cloud. The Nest thermostat has higher processing capacity for the artificial intelligence that gives them intelligence.

(a) Interoperability

Internet of Things is made possible by the expansion of network connectivity to previously isolated devices. The connectivity of these things is crucial because even basic interactions between devices add to the IoT network's collective intelligence. It makes the devices compatible with and accessible across a network. Connecting smart devices and software opens up new possibilities for the Internet of Things business. Adding a WiFi module and calling it a day doesn't cut it when it comes to connectivity in the IoT. Network accessibility and compatibility are both facilitated by connectivity. Connecting to a network constitutes accessibility, whereas compatibility guarantees the shared capacity for receiving and sending information. This is nothing more than Metcalfe's Law, and it holds true for the Internet of Things [7].

**Nature of change**

The basic function of IoT devices is to observe and record the dynamic changes occurring in their surroundings. The devices' states, such as being asleep or awake, connected or disconnected, and in what environmental conditions (such as temperature, location, and velocity) are constantly shifting. Both the total number of devices and their distribution in time, space, and individuals are subject to constant flux. Devices' states (such as being asleep or awake, connected or disconnected, and so on) and their surroundings (such as their location and velocity) are always in flux. Furthermore, the number of devices is dynamic and might vary at any time [8].

**d) Extreme size**

Compared to the number of devices currently linked to the Internet, the number of devices that will need to be managed and communicate with each other will be significantly larger. The need of properly managing and interpreting data produced by such devices for practical use grows. An estimate report by Gartner (2015) verifies the massive scope of IoT, predicting that 5.5 million new objects will be connected every day and 6.4 billion connected devices would be in operation worldwide in 2016, an increase of 30% from 2015. According to the research, there will be 20.80 billion Internet-enabled gadgets in use worldwide by the year 2020.When compared to the number of devices currently linked to the Internet, the number of devices that will need to be controlled and communicate with each other will be at least an order of magnitude bigger. The analysis of the data and their management for practical use will be of even greater importance. This has implications for both the meaning of data and the effectiveness of data processing.

(3) Perceiving without sensors to detect or measure environmental changes, there would be no Internet of Things to report on the state of or interact with. The capabilities that accurately reflect an understanding of the physical world and the people living in it can be developed with the help of sensing technologies. Sensing data is analog input from the real world, yet it can yield profound insights into the complexities of our universe. As a species, we have a propensity to take our senses and the ability to comprehend our surroundings for granted. With the use of sensing technology, we can design experiences that accurately represent our understanding of the real world and the people living in it. Even though it's just the analog input from the physical world, it may provide a lot of light on our complicated universe.

(e) Variation one of the distinguishing features of the Internet of Things is its inherent heterogeneity. IoT devices operate on a wide variety of network and hardware architectures,

allowing them to communicate with one another and with service platforms. The ideal design for the Internet of Things would allow for seamless network communication between disparate systems. Scalability, modularity, extensibility, and interoperability are essential design needs for heterogeneous items and their contexts in the Internet of items. The devices that make up the IoT are diverse because they run on many operating systems and network topologies. Through various networks, they are able to communicate with other devices and service platforms [9].

F) Safety Security flaws in IoT devices are a fact of life. It would be a mistake to ignore security risks related to the IoT as we gain efficiency, new experiences, and other benefits from it. The Internet of Things raises serious concerns about data security and personal privacy. Developing a security paradigm is essential for protecting information across endpoints, networks, and transmissions.

**Applications of Internet of Things (Iot)**

Some useful applications of Internet of Things (IOT) are:

a. Connected Health
b. Smart City
c. Connected Cars
d. Smart Home
e. Smart Farming
f. Smart Retail
g. Smart Supply Chain

**Connected Health (Digital Health/Tele health/Telemedicine)**

Medical applications of IoT range from advanced and smart sensors to equipment integration to remote monitoring devices. It may help doctors save lives and keep patients healthy by enhancing the quality of treatment they provide. The Internet of Things in healthcare can increase patient engagement and happiness by giving people more time to talk to their doctors. IoT in healthcare offers new, cutting-edge tools to the ecosystem, from personal fitness sensors to surgical robots, all of which contribute to the improvement of medical care overall. The Internet of Things is transforming the healthcare industry by offering low-cost options for both patients and doctors. [10].

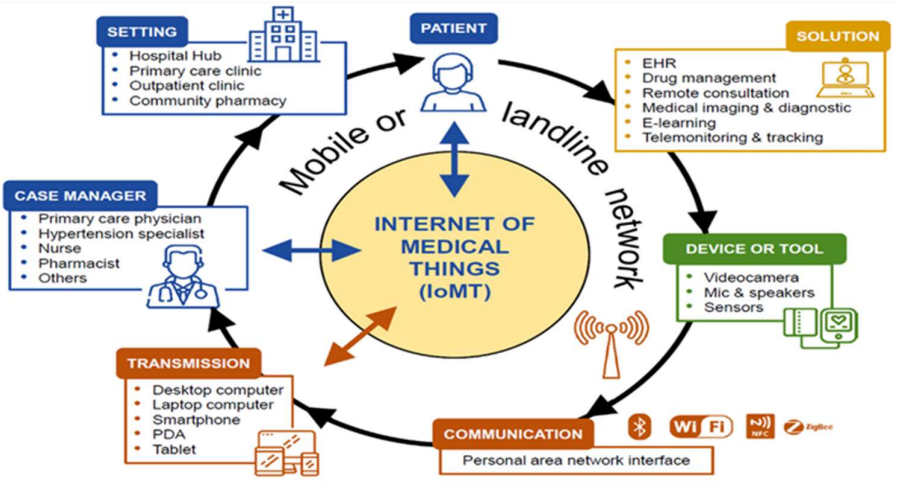


**Figure 1: Connected Health**

Healthcare connectivity is still a relatively untapped area for IoT implementations. There is tremendous promise for both businesses and society at large in the idea of a connected healthcare system and smart medical devices. The use of IoT in healthcare is expected to explode in the near future. The Internet of Things (IoT) in medicine aims to give patients more control over their health by allowing them to use linked devices. The obtained data will aid in individualized analysis of health status and the development of specialized plans of action to counteract disease. The video below demonstrates how the Internet of Things (IoT) can change the face of healthcare forever.

"Smart City"

The concept of the "smart city" is another intriguing use of the Internet of Things. Internet of Things applications for smart cities include intelligent surveillance, energy management systems, automated transportation, water distribution, urban security, and environmental monitoring. The Internet of Things will provide answers to some of the most pressing issues city dwellers experience today, such as air and traffic pollution, gridlock, and power outages. Smart Belly garbage cans, which use cellular connectivity, will notify the proper authorities when it's time to empty the can [11].


**Figure 2: Smart City**

Residents can locate open parking spots throughout the city with the use of sensors and online apps. The sensors can also identify flaws with the electricity system, such as tampered meters, general malfunctions, and improper installation.

b) Vehicles With Internet Connections

Optimizing the vehicle's internal systems has been a primary goal of automotive digital technology. However, recent years have seen a shift in focus toward bettering the time spent behind the wheel. Using on-board sensors and internet connectivity, a "connected car" can improve its own performance, maintenance, and passenger comfort. The vast majority of established automakers, along with a few bold upstarts, are developing connected vehicle solutions. Tesla, BMW, Apple, and Google are just a few of the major companies working on the next automotive revolution [12].

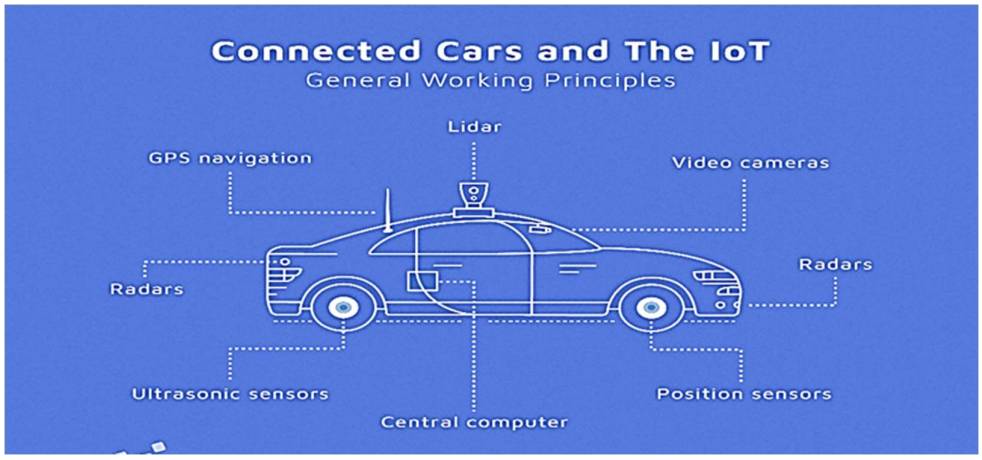


Figure 3: Connected Cars

In order to traverse the modern environment, connected vehicles rely on a vast and complicated network of sensors, antennae, embedded software, and other technologies. Decisions must be made quickly, accurately, and consistently by it. It must be trusted as well. When people give up full control of the steering wheel and brakes to the autonomous or automated vehicles already being tested successfully on our roadways, these requirements will become much more pressing.

**b) High-Tech House**

Smart houses are expected to become as prevalent as smartphones, and they have already become a revolutionary step toward that goal in the domestic market. Smart homes consistently top the list of IoT applications across all channels because they are the most important and efficient. Over $2.5 billion has already been invested in Smart Home startups, and that number is expected to expand rapidly. Who wouldn't want to turn on the air conditioner before they got home or turn out the lights after they left? Or, if you're away, you can give friends temporary access by unlocking the doors. As the Internet of Things develops, it shouldn't come as a surprise that manufacturers are creating items to improve your quality of life.

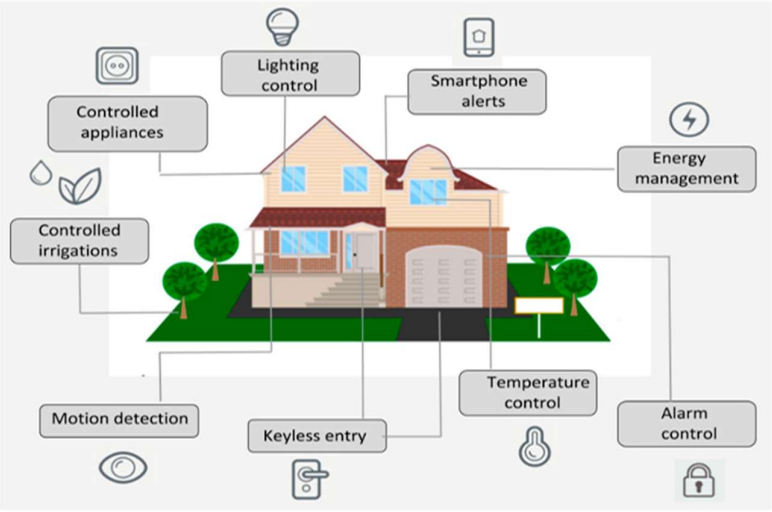


**Figure 4: Smart Home**

Homeownership is the single largest financial commitment most people will ever make. Products for the "smart home" claim to save down on expenses in all three areas. Companies like Nest, Ecobee, Ring, and August (to name a few) are hoping to become household names by providing a smart home experience unlike anything consumers have ever had before [13].

Smart Farming

One area where the Internet of Things could be useful is in smart farming. However, the Internet of Things can transform farming in part because it can monitor the vast number of farming activities located in remote areas and the massive number of cattle that farmers labor on. However, there hasn't been widespread interest in this concept just yet. However, it's still one of the most important uses of the Internet of Things. Particularly in agricultural-product exporting countries, "smart farming" has the potential to become a significant application field.

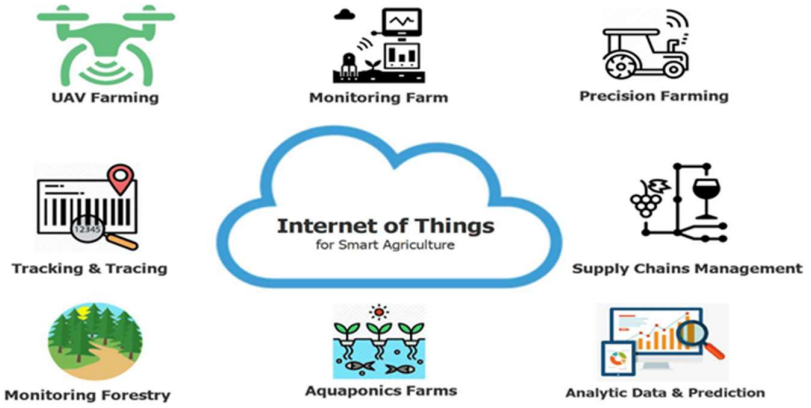


Figure 5: Smart Farming

Increasing sales, decreasing theft, facilitating inventory management, and better serving customers are just a few of the many ways in which Internet of Things (IoT) solutions and IoT embedded systems are being adopted by smart retailers. With the help of the Internet of Things, traditional stores can better compete with their digital counterparts. They can win back customers and increase sales by offering discounts and incentives to shop in their stores [14].


Figure 6: Smart Retail

Internet of Things has tremendous promise in the retail industry. With the help of IoT, stores may improve their consumers' in-store experiences by connecting with them on a personal level. Keeping in touch with customers even when they're not physically in the business will

be possible thanks to smartphones. Bettering the shopping experience for customers with mobile communication and Beacon technologies. Customers' movements in a store can be monitored, allowing for strategic placement of high-demand items.

**An Intelligent Supply Chain**

For the past few years, supply networks have been gradually becoming more intelligent. Popular services include those that allow businesses keep tabs on their shipments at all times, wherever they may be, and those that facilitate the sharing of inventory data between suppliers. Embedded sensors in manufacturing equipment can transmit information regarding pressure, temperature, and machine utilization in an IoT-enabled system. Workflow processing and adjustments to equipment settings for maximum efficiency are also under the IoT system's purview [15].

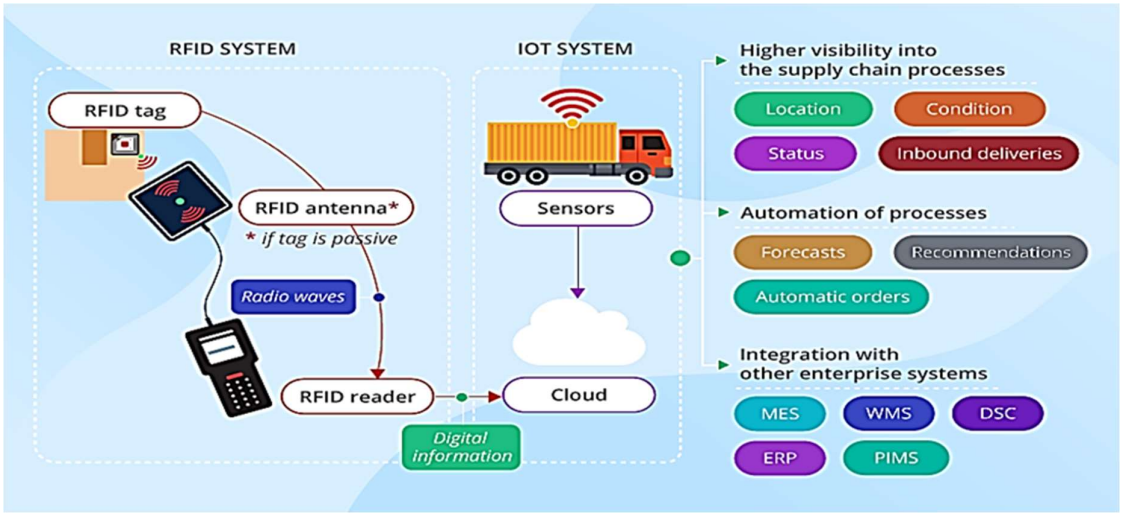


Figure 7: Smart Supply Chain

The Problems with Iot Security Internet of Things security involves keeping IoT devices safe from harm. Many business owners understand the importance of installing antivirus software on their PCs and mobile devices, but IoT devices are often overlooked when it comes to security.

There is no escaping the prevalence of IoT gadgets. Everything from refrigerators and automobiles to monitoring equipment on production lines is getting wired into the internet. The expansion of the Internet of Things sector is mind-boggling. By 2022, Juniper predicts, there will be more than 50 billion sensors and gadgets connected to the internet.Businesses are eager to adopt IoT devices due to their high potential for savings, just as consumers are quick to reap the benefits of lifestyle-enhancing IoT gadgets. By integrating Internet of Things (IoT) devices into every stage of production, Harley-Davidson was able to cut costs by 7% and boost net margin by 19% at its'smart factory' in York, Pennsylvania.

**a) Confidence in the Data**

Through the IoT, a vast ecosystem consisting of billions of individual devices is brought together. If one data point is tampered with, it will affect all of the data that is passed between the sensor and the master server. Integrity can only be maintained through the use of a decentralized distributed ledger and digital signatures [16].

**(b) Capabilities for Using Encryption**

The process of encrypting and decrypting data is ongoing. Sensors in the Internet of Things network still can't process data. Firewalls and physically isolating devices on different networks can protect against brute-force attacks.

**d) Concerns About Personal Information**

Sharing information between networks, devices, and users is key to the Internet of Things. Smart devices collect data for a variety of purposes, including enhancing efficiency and user experience, facilitating decision making, enhancing service quality, etc., so it's imperative that this data is kept safe and secure all the way to its final destination.

**(d) Shared Schematic**

Due to the lack of a universal framework, each manufacturer must independently handle matters of security and confidentiality. When a standardized framework is put in place, everyone's work may be put to use in a scalable way, allowing for code reuse [17-21].

**Conclusion**

The Internet of Things structure can be penetrated at any level. As a result, there is an abundance of security hazards and regulations that must be dealt with. Authentication and access control protocols may be where most IoT research efforts are currently directed, but as technology advances, it will be necessary to unify new networking protocols like IPv6 and 5G in order to realize the progressive mash up of IoT topologies. This chapter's primary goal was to draw attention to the critical security challenges of the Internet of Things (IoT), with an emphasis on the security assaults and their respective mitigation strategies. Many Internet of Things (IoT) devices become easy targets because they lack adequate security mechanisms, and the victims often are unaware that they have been compromised. Confidentiality, integrity, authentication, and similar topics are covered in this chapter's discussion of security needs. In this paper, we'll look at some of the many ways IoT can be put to use. To better understand the dangers and their attributes from various intruders like organizations and intelligence agencies, this article aims to help experts in the security industry identify the most pressing problems in IoT security.

a) Robotics

Eventually, businesses will need to manage a plethora of Internet of Things gadgets. It can be challenging to keep track of this massive volume of user information. It is undeniable that a breach of even a single algorithm might compromise the entire data infrastructure.

(b) Refreshments

A strict protocol must be followed while updating millions of devices. Unfortunately, not all devices can be updated wirelessly and must instead be updated manually. One must monitor the availability of updates and implement them on all of the various devices. This becomes a tedious and complicated procedure, and any errors made at this time could result in security flaws in the road. Security Currently, investments in safeguarding infrastructure and networks are not prioritized as they should be. The Internet of Things relies on millions of data points, all of which must be protected. The requirement for multi-layer security, or security at every level, is undeniable. Every component of an IoT solution, be it an endpoint device, cloud platform, embedded software, or web/mobile application, must be secure. Security is complicated by the wide variety of devices involved.

**References**

1. R.Vignesh and 2A.Samydurai ans1 Student, 2Associate Professor Security on Internet of Things (IOT) with Challenges and Countermeasures in 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939.
2. N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, 203-209, 1987.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. J. S. Kumar and D. R. Patel, “A survey on internet of things: Security and privacy issues,” International Journal of Computer Applications, vol. 90, no. 11, 2014.
10. 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.
11. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,”IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.
12. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,”Comput. Netw. vol. 54, no. 15, pp. 2787–2805, Oct 2010.
13. M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the internet of things,” in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.
14. L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,”IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
15. L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santana, “Internet of things in healthcare: Inter-operability and security issues,” in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.

16. Mohan, “Cyber security for personal medical devices internet of things,” in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374.
17. S. De, P. Barnaghi, M. Bauer, and S. Meissner, “Service modelling for the internet of things,” in Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on. IEEE, 2011, pp. 949–955.
18. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions, “Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
19. M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, “From today’s intranet of things to a future internet of things: a wireless-and mobility-related view,” Wireless Communications, IEEE, vol. 17, no. 6, pp. 44–51,2010.
20. C. Hong song, F. Zhongchuan, and Z. Dongyan, “Security and trust research in m2m system,” in Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on. IEEE, 2011, pp. 286–290.
21. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, “Trust in m2 communication,” Vehicular Technology Magazine, IEEE, vol. 4,no. 3, pp. 69–75, 2009.