IJCSMA
Pratham Sharma *et al*, International Journal of Computer Science and Mobile Applications,
Vol.10 Issue. 9, September- 2022, pg. 33-40 **ISSN: 2321-8363**
Impact Factor: 6.308
(An Open Accessible, Fully Refereed and Peer Reviewed Journal)

Future Direction of Internet of Things (IoT) and it's Challenges in Application Domain

Pratham Sharma[1]; Pratyush Kumar Jha[2]; Anirban Bhar[3]; Tamasree Biswas[4]
[1,2]B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India
[3,4]Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India
[1] ps1452003@gmail.com
[2] pratyushkumarjha2001@gmail.com
[3] anirban.bhar@nit.ac.in
[4] tamasree.biswas@nit.ac.in

DOI: 10.5281/zenodo.7088950

Abstract

It is essential to understand the many potential domains for IoT applications and the research difficulties that are related to these applications as the Internet of Things (IoT) increasingly develops as the next stage of the Internet's evolution. IoT is anticipated to permeate practically every facet of daily life, from smart cities to smart surroundings to smart living and smart environments to smart health care, smart agriculture, logistics, and smart retail. Despite recent significant advancements in IoT enabling technologies, there are still a lot of issues that need to be fixed. Numerous research difficulties are sure to emerge since the Internet of Things notion results from diverse technology. The Internet of Things (IoT) is a key research issue for studies in many related domains, including information technology and computer science, due to its broad scope and impact on nearly every aspect of our life. IoT is therefore opening up new avenues for the conduct of research. In addition to discussing upcoming applications and research problems, this presentation analyses the recent progress of IoT technology.

Keywords: Internet of Things, Cyber Attacks, Virtualization.

1. Introduction

The Internet of Things (IoT) is an interconnected system of uniquely addressable physical items with varying degrees of processing, sensing, and actuation capabilities that share the capability to interoperate and communicate through the Internet as their joint platform [1]. The Internet can be described as the communication network that links people to information. As a result, the major goal of the Internet of Things is to enable connections between objects and people at any time or location via any network, method, or service. The Internet of Things (IoT) is increasingly being seen as the next stage in the development of the Internet. IoT will make it possible for common gadgets to be connected to the internet in order to accomplish a wide range of different objectives. Only 0.6% of potential IoT devices are believed to have been connected as of this writing [2]. But it's likely that more than 50 billion gadgets will have internet access by the year 2020.

IoT functions as a network of various "connected" devices and a network of networks [3], as shown in Fig. 1, while the internet has evolved to become more than just a simple network of computers and has instead become a network of varied devices. These days, a wide range of gadgets, including smartphones, cars, industrial systems, cameras, toys, buildings, home appliances, and countless more, may all communicate information online. These devices can perform smart reorganisations, tracing, positioning, control, real-time monitoring, and process control regardless of their sizes and capabilities. The number of gadgets that can connect to the Internet has significantly increased in recent years. Even while the consumer electronics industry has seen its biggest financial impact, namely the rise of smartphones and interest in wearable technology (watches, headsets, etc.), connecting people has only become a small part of a larger trend towards the merging of the physical and digital worlds.

With all of this in mind, it is anticipated that the Internet of Things (IoT) will keep growing in terms of the range of devices and operations it can support. This is seen from the word "Things'" vagueness, which makes it challenging to define the IoT's expanding boundaries [4]. The Internet of Things (IoT) constantly presents a seemingly infinite supply of prospects, not just in enterprises but also in research, even as commercial success continues to materialise. In light of this, the article discusses the many IoT domain applications that could be made as well as the accompanying research hurdles.

2. Related Work

In 1991, Mark Weiser published "Ubiquitous Computing," which was his description of the future Internet. He was primarily concerned with how to activate the intelligent dwelling environment in the presence of mobile phone technology, which offers a potent multimedia system [5]. One of the pioneers who has spoken about IoT is Kevin Ashton [6]. Atzori A.lera et al. [7] divided the Internet of Things into three paradigms: the internet-oriented (Middleware), the things-oriented (Sensors), and the semantic-oriented (Semantic Web) (Knowledge). In his book "When Things Start to think" published in 1999, Neil Gershenfeld discussed related topics from the MIT Media Lab at the Massachusetts Institute of Technology.

To create the Electronic Product Code (EPC) and use RFID to identify items on the network, Auto-ID Labs and MIT set out in 1999. IoT started to appear in book titles for the first time in 2003–2004 with the rise of initiatives supporting the concept, including Cooltown, Internet0, and the Disappearing Computer effort. The US Department of Defense extensively disseminated information about RFID deployment. When the International Telecommunication Union ITU published its first report in 2005, the Internet of Things (IoT) reached a new level. In order to promote the use of Internet protocol (IP), activate the IoT concept, and form the IPSO Alliance, a collection of businesses including Cisco, Intel, SAP, and over 50 others got together in 2008. IoT was "Born" by Cisco's Internet Business Solutions Group (IBSG) in 2008-2009 [8]. IoT can be defined from the aforementioned views as a collection of intelligent things/objects, such as household appliances, mobile devices, laptops, etc., that are connected to the Internet through a single framework, which could be cloud computing.

The best architecture design serves as a cornerstone for the construction of a privileged IoT system. This architecture helped to handle many problems with the IoT environment, including scalability, routing, networking, etc. The three primary dimensions that typically make up the IoT architecture approach are:

Information items, also known as sensing, identifying, and control items, are included in the IoT environment. Independent networks, which have features like self-configuration, self-protection, self-adaptation, and self-optimization, are also included. Finally, intelligent applications, which have intelligent behaviour over the Internet generally, are included. The point where these dimensions meet produces a

"Infrastructure of IoT" is a new field that provides systems to support the special items and can offer a range of services, including data protection, location identification, and commodities identification.

In order to establish an IoT application, the preferred architectural method is based on an open architecture, the EPC worldwide network, and the article will focus on two types, namely, architecture called "EPC global network" and another called "Unite and ubiquitous IoTs or U2IoTs". The RFID technology plays a critical role in differentiating between these mobile objects in the system created by AutoID Center and dubbed "the EPC global network." This system conveys dynamic information about objects and things to offer authorised users with a history of the product movement. The IoT bases its architecture framework design on the EPC global network [9].

Connecting the physical, digital, and social worlds is a goal of the IoT's future architecture. U2IoTs, also known as Unite and Ubiquitous IoTs, are an alternative type of IoT architecture that combines the physical and digital worlds. The U2IoTs is made up of a variety of heterogeneous systems, such as an IoT unit designed to resemble a human neural network and offer solutions for particular applications. It also includes the industrial IoT, local youth IoT, national IoT, and global IoT, which combine multiple Unit IoTs with ubiquitous features. It is similar to the social organisation framework. The U2IoT model's key features are social coexistence, cyber and physical coexistence, connectivity and interactivity, space-time consistency, and multi-identity status.

This position cannot be justified based on prior knowledge of the IoT environment since there are two main reasons to reject it. Due to the nature of IoT, which requires lightweight communication protocols, IP may not always be used to address objects. In particular, when working with clever little things, the complexity of the TCP/IP protocol is inappropriate. In contrast to traditional networks, the IoT environment is primarily focused on connected smart items. They do this because doing so moves them beyond simply being an Internet extension. The development of interoperable systems also affects how the Internet of Things behaves [9].

3. IoT Architecture and Technology

All of the functionalities of IoT systems are defined by the five key layers that make up the IoT architecture. These layers include the business layer, the network layer, the middleware layer, and the application layer. The perception layer, which comprises physical devices like sensors, RFID chips, barcodes, and other physical items connected to an IoT network, is at the base of the IoT architecture. Information is gathered by these devices and sent to the network layer. The information is transmitted from the perception layer to the information processing system using the network layer as a transmission medium. This information transmission may employ any wired or wireless technology, including 3G/4G, Wi-Fi, Bluetooth, and others. Middleware layer is the layer below that. This layer's primary responsibility is to process the data obtained from the network layer and make judgments in light of the outcomes of ubiquitous computing. The application layer uses this processed data after that for worldwide device management. A business layer that controls the complete Internet of Things system, its applications, and services is present on top of the architecture. The business layer further uses this knowledge to develop future goals and objectives by visualising the data and analytics it receives from the application layer. The IoT architectures can also be altered based on the requirements and application domain [10][11][12].

In addition to a layered foundation, an IoT system is made up of a number of functional building blocks that enable different IoT functions such sensing mechanisms, authentication and identity, control, and management [13]. Figure 1 depicts these essential IoT architectural building pieces.

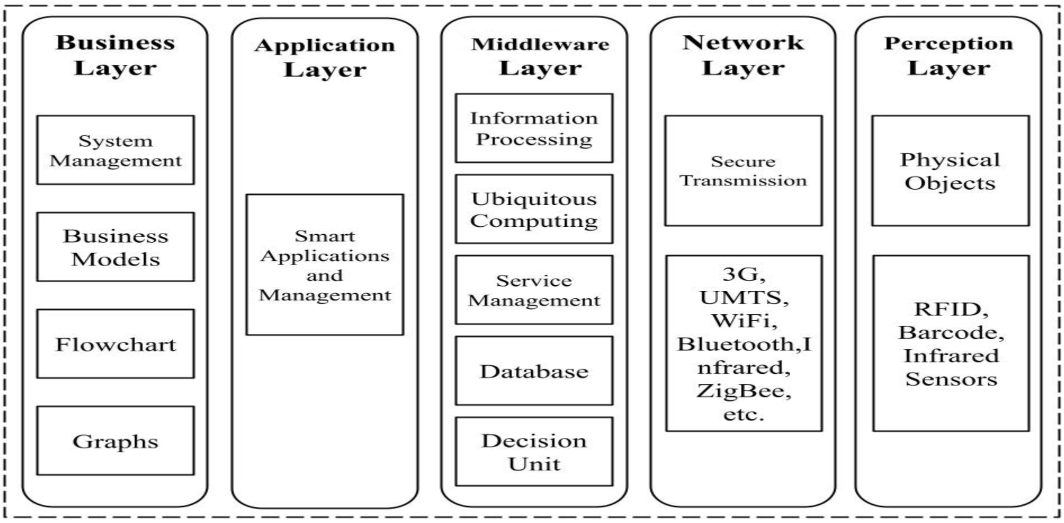

Figure 1: Five-Layers Architecture

Members of the RFID community served as the original inspiration for the Internet of Things when they discussed the possibility of learning more about a tagged object by looking up a website address or database entry that corresponds to a specific RFID or Near Field Communication technology. IoT's essential technologies, which are featured in the research paper "Research and application on the smart home based on component technologies and Internet of Things," are RFID, sensor technology, nanotechnology, and intelligence embedded technology. Among them, RFID serves as the framework and networking heart of the Internet of Things [14]. Users were able to bring physical things into the cyberspace thanks to the Internet of Things (IoT). Different tagging technologies, such as NFC, RFID, and 2D barcode, made it possible for physical items to be identified and referred to online [15]. The Internet of Things, or IoT, is a network that is built on the always available hardware resources of the Internet and combines Internet-connected items with sensor and radio frequency technology. Since the application of computer fields, communication networks, and worldwide roaming technology had been applied, it is also a new wave of the IT sector. In addition to highly advanced computer and communication network outside technologies, it also includes numerous new Internet of Things supporting technologies, such as information collection, remote communication, remote information transmission, and sea measures information intelligence analyses and controlling technology, among others [16].

4. Application Domain of IoT

The Internet of Things (IoT) is now a comprehensive business transformation plan rather than just a connection strategy. Industry leaders are gradually getting new possibilities to develop products and services that were previously thought to be unachievable.

The four IoT maturity stages—Data Generation and Ingestion, First Analytics, Deep Learning, and Autonomous Decision Making—were covered in the preceding article. The pace of sustainable company growth, including higher profitability for enterprise executives, has been accelerated by the IoT maturity journey.

Enterprise leaders have only recently realised how critical the Internet of Things is to their organisations.

92% of them, according to a McKinsey & Company survey, think that IoT would improve their goods and operations by 2020.

This is the tipping moment that will guarantee that IoT technology develops to produce genuinely seamless, connected experiences. IoT technology is used by a wide range of businesses, all of which are typically in different phases of development. Some are just getting started, concentrating on making sure everything is linked or integrated. Others, meantime, are working to create a more integrated business model for their company's operations.

To better understand how the Internet of Things is affecting businesses and transforming lives, we provide the top IoT real-world applications from across 7 super-domains here:

4.1 Smart Homes

The IoT-driven, technologically enhanced institution that rules the world is the smart home. By giving smart devices additional features and capabilities, IoT drives the smart home. The potential of the smart home for consumer convenience, safety, and time savings has consumers enthralled.

A Statista analysis projects that by 2022, the worldwide smart home market will be worth 53 billion US dollars.

As investments in smart home technologies increase, the distinctions between market giants are becoming less distinct. Smart Homes and IoT technologies are now widely used due to the rising demand for linked assets, security systems, room control, energy management, and light control.

4.2 Wearables

The adoption of wearables is increasing more quickly. There are several wearable items available, including smart apparel, GPS tracking belts, and fitness tracking brands. These gadgets are always changing to provide smaller and more energy-efficient options throughout time.

For instance, health and fitness-focused wearables provide biometric measures like heart rate, sweat content, and blood oxygen levels.

Forbes estimates that 411 million wearables will be sold worldwide in 2020.
This IoT technology's consumer-focused side will undoubtedly add tremendous value to our lives.

4.3 Smart Cities

IoT-enabled smart cities can be used in a variety of different contexts. IoTs have lowered energy costs, helped to create a healthier environment, improved traffic management, increased public safety, and optimised street lighting. These benefits extend to smart lighting, smart parking, connected public transportation, and waste management.

4.4 Smart Grids

Internet of Things-based smart grid technologies meet the energy needs of the modern world. In order to balance out the growing complexity of the energy distribution networks and get real-time visibility into the consumption process, they have developed a workable solution.
Smart back-end systems and internet-connected sensors can supply real-time data to build more responsive and efficient systems.
As an illustration, metres and substations can virtually connect to one another as well as to business vehicles and employee devices using IoT apps. Realized efficiencies will result from such linkage.

4.5 Industrial IOT (IIoT)

The Industrial Internet of Things (IIoT) is supplying businesses with cutting-edge sensors, software platforms, and programmed resources to build futuristic infrastructure. Big data analytics are used by IIoT to interface with industrial data and produce more reliable findings. This enables businesses to maximise production by dealing with process inefficiencies effectively and identifying issues early.
By 2030, IIoT, according to Accenture, may boost the global economy by $14.2 trillion.
Applications of the IIoT include inventory management, wearable technology like industrial smart glasses, remote monitoring and control of operations utilising network-connected sensor data, and equipment and tools with integrated sensors.

4.6 Connected Cars

The automobile industry is fervently pursuing IoT to enable optimal and unrestricted operation of vehicles. The improved IoT potential has inspired auto engineers to work harder on developing the in-car experience.
By 2020, there will be 220 million linked automobiles on the road, predicts Business Insider.
Everyone is thrilled about the linked cars phenomenon, from automakers to software providers. Based on the inputs and sensors that have been previously saved, a connected car may handle its own operations.
The cloud can be used to exchange and receive data from vehicles that are outfitted with cameras, sensors, and mobile connectivity. With that information, the options are unlimited. Automotive IoT fundamentally transforms the auto industry, including location monitoring, in-car content and services, GPS-based navigation, fleet management, and driver assistance.

4.7 Smart Supply Chain

IoT technology offers a useful strategy to advance supply chain management. In order to manage commodities from any location, at any time, on a worldwide scale, the logistics and transportation sector has begun utilising comprehensive IOT solutions.
IoT sensors provide a clear view of how the product is being handled on its trip from the manufacturing facility to the point of consumption via the complete logistics network.
When it comes to fleet management, automated warehouse operations, and cargo integrity monitoring, logistic providers can reach a higher degree of operational efficiency, transparency, and streamlined processes.

5. Cyberthreats and it's Countermeasures

IoT undoubtedly improve our current infrastructure. But it heavily relies on security. As the implementation of IoT in our current infrastructure means it will be managing telecommunication, water and energy networks, government infrastructure and so on. A digital attack on this network can cause large scale cyber-attack as this device are interconnected.

Phishing attacks- It is a type of cyber-attack where attacker pose as trusted entity to trick users to steal their personal information through the means of fake website or malicious websites. The primary objective of these attackers is to control the operating system that is linked with IoT system by using techniques such as link manipulation, filter evasion, zero days malware and so on.

There are few ways to counter it. To automatically detect and analyse phishing attack, Madhusudhanan et al. proposed a new technique called PHONEY. It provides information on qualities of the sites, security certificate, information related to having malicious code and misleading URL.

It sits between user's mail transfer agent (MTA) and mail user agent (MUA) and process each mail for phishing attack.

DOS (Denial of Service)- It is a cyberattack where the attacker seeks to shut down the services of a network or machine to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending information to the site that triggers a crash. It could prove a major inconvenience in the future if society were to depend upon IoT.

We can use machine learning to detect any intrusion in the network using techniques such as PCA. It's a feature reduction technique that converts a number of probably correlated features into reduced uncorrelated ones which are called principal components. It can reduce the complexity of the model. Modern security technologies have also developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS (Distributed Denial of Service), it is still regarded as an elevated threat and is of higher concern to organizations and countries that fear of being targeted by such an attack.

Man in the middle-A man-in-the-middle (MiTM) attack is a mischievous type of cyber-attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications e-commerce sites and other websites where logging in is required.

We can counter this by using blockchain security architecture. Blockchain is a chain of block which contains information. It was proposed in 1991 and implemented in bitcoin architecture in2009 by Satoshi Nakamoto. These blocks contain three main things: Data, Hash of the block and Hash of the previous block. A hash is a unique code which depend upon the content of the block and its complete unique to the block. Tampering with the block changes the hash which and the next block cannot detect ot any longer. Along with the help of proof of work and a distributed person to person network and smart contracts. I t becomes nearly impossible to hack it.

Botnet- It is a large-scale cyber-attack where a group of Internet connected devices inflected with malwares(bots) which are remotely controlled by an attacker and then carry out cyber-attacks. It is a kind of a robotic network attack in which the owner can control the botnet using command and control(C&C) software.

Using random forest, we can detect these botnets. Random forest is an ensemble classifier that produces many decision trees using a sample subsets and randomly selected variables. It has 100% precision and high computational efficiency. It can handle multiple botnets at time.

Ransomware: This type of cyber-attacks are DoS attacks using malicious code injection in the user target data using cryptography techniques until the ransom is fully paid. IIOT (Industrial Internet of Things) gateways are very vulnerable to the ransomware attack. These gateways act as a bridge between perception layer and network layer. If the attack is successful, the attacker can alter the gateways password and updating the existing firmware with the malicious one. It can also access and encrypts all the user and data files.

We can use Deep Neural Networks (DNN) to detect ransomware. DNN is a complex neural network which uses sophisticated mathematical modelling to process data in complex ways. A DNN is constructed with the analysis of network behaviour in ransomware and trained on critical payloads selected from packets. This method is designed to detect the infection as soon as possible and can be used in real life network architecture. It has a detection rate a precision of over 90%.

6. Conclusion

The future is full of interdependent technologies which will enhance the living of humanity in a very different way. It will create a new base for insane ideas which will help humans to understand more about themselves and the nature. It will eliminate the hurdles that are coming now to interact and operate a certain thing at every level. Faster approach, lower cost and effective management of entities, environments and products will boom the lifestyle and economy. IoT enables speedier and better quality of monitoring, processing, controlling when needed. It will generate paths to earn billions of dollars of income which we can't imagine now and ultimately our society will be heavily benefitted by this interconnected tech.

As India is a developing country, it has a wide IoT scope. According to Naukri.com, the future scope of IoT in India is very high as there are 117,114 job openings for an IoT Developer here. On the other hand, in the United States, the demand for an IoT Developer has jumped over 300 percent.

Smart cities will be then possible to create with the help of IoT. Connected cities can change the life of its citizens, by providing better traffic management, connected cars for an easy commute, smart garbage for waste management, and even to improve air quality. So, it is important that we make this tech more advance and give its benefits to everyone.

References

[1] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)", in 2015 Internet Technologies and Applications (ITA), pp. 219– 224, Sep. 2015, DOI: 10.1109/ITechA.2015.7317398.
[2] P. J. Ryan and R. B. Watson, "Research Challenges for the Internet of Things: What Role Can OR Play?," Systems, vol. 5, no. 1, pp. 1–34, 2017.
[3] M. Miraz, M. Ali, P. Excell, and R. Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", Future Internet, vol. 10, no. 8, p. 68, 2018, DOI: 10.3390/fi10080068.
[4] E. Borgia, D. G. Gomes, B. Lagesse, R. Lea, and D. Puccinelli, "Special issue on" Internet of Things: Research challenges and Solutions".," Computer Communications, vol. 89, no. 90, pp. 1–4, 2016.
[5] Daoliang Li, Yingyi Chen, Oct. 2010, Computer and Computing Technologies in Agriculture. Springer, 24-31.
[6] InternetofThings,2015http://www.rfidjournal.com/article s/view?4986.
[7] L. Atzori, A. lera, G. Morabito, The Internet of Things: Survey. Computer networks, 2787–2805.
[8] Internet of Things, 2014 http://postscapes.com/internet- of-things-history.

[9] Nihong Wang, Wenjing Wu, 2012 The Architecture Analysis of Internet of Things, Computer and Computing Technologies in Agriculture V IFIP Advances in Information and Communication Technology, 193-198.

[10] Olivier F, Carlos G, Florent N. New security architecture for IoT network. In: International workshop on big data and data mining challenges on IoT and pervasive systems (BigD2M 2015), procedia computer science, vol. 52; 2015. p. 1028–33.

[11] Luk M, Mezzour G, Perrig A, Gligor V. MiniSec: a secure sensor netowrk communication architecture. In: Proc: 6th international symposium on information processing in sensor networks, Cambridge, MA, USA, 25–27 April 2007.

[12] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst. 2013;29(7):1645–60.

[13] Sebastian S, Ray PP. Development of IoT invasive architecture for complying with health of home. In: Proc: I3CS, Shillong; 2015. p. 79–83.

[14] Gigli, M. and Koo, S. (2011) Internet of Things, Services and Applications Categorization. Advances in Internet of Things, 1, 27-31. http://dx.doi.org/10.4236/ait.2011.12004

[15] (2005) ITU Internet Reports, International Telecommunication Union. The Internet of Things: 7th Edition. www.itu.int/internetofthings/on

[16] Want, R. (2006) An Introduction to RFID Technology. IEEE Pervasive Computing, 5, 25-33