Modern technology advancement in Internet of Things (IoT)

[1]Dr. Abhishek Kumar, [2]Dr. Ashok Gupta, [3]Neha Rani, [4]Dr. S.S. Chauhan
[1,2,3] Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
[4]NICE School of Business Studies, Faculty of Management Studies, Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- [1]abhishekkumar@shobhituniversity.ac.in, [2]dr.ashok@shobhituniversity.ac.in
[3]neharani@shobhituniversity.ac.in, [4]sschauhan@shobhituniversity.ac.in

Abstract: The Internet of Things (IoT) is a constantly evolving field for data sharing and communication, and from this current reality objects such as actuators, RFIDs, sensors, machines, and other similar devices, each of which has its own framework for data sharing, data processing, and communication, are emerging. The Internet of Things (IoT) brings brilliance to the interior of connected things, allowing for better decision-making, communication, serviceability according to demand, and information exchange. Currently, millions of things as objects are linked together via a variety of media, generate data in a variety of forms, and operate according to a variety of business models in order to provide a variety of services. As a result, heterogeneity in design, network protocols used by objects or things, and data generated by objects or things raise a number of challenges such as privacy and security concerns, network complexity, standardisation, scalability, and so on. This article provides a high-level overview of the Internet of Things (IoT) problems and issues, as well as the prompting technologies that may be used in conjunction with IoT to provide solutions to these challenges and issues.

Keywords: Internet of Things, IoT Architecture, Network, Security, Sensors.

1. INTRODUCTION

Transformation is just one ongoing aspect in our world. Smaller technological advancements are changing the lives and way of life of people. For example, in earlier years, there were no telephone gadgets, people were trying to share information or interact with each other through letters. As the telephone innovation became widespread, human existence altered. Individuals can communicate effectively from home and then cellular telephones come in, where people can communicate from everywhere. Similarly, the Internet of Things (IOT) is the newest technology of this century to make today's lives simpler and pleasant for people. The technology itself implies that it is mostly utilised to link the various things and to provide an extensive degree of services for the organisation and the community. IOT thus provides a stage for devices not only to interact with one another, but also to facilitate computation, feeling and processing every time from anywhere, via the connection of various gadgets [1].

IOT provides many kinds of technology, which may be utilised in diverse areas such as agriculture, factories, domestic automation, transportation, healthcare, etc. IOT offers many advantages and simplifies and relaxes human life, but also poses several difficulties with the development of associated network equipment. The expansion of associated systems rates will promote energy use to elevate environmental CO_2 emissions, accessibility issues, protection and protection of mutual information, standardisation of different devices, network sophistication, content heterogeneity, interoperability of related devices produced by and employed by the various communications protocols, etc. This article is organised into a few sections in which it covers the IOT architecture and basics, the current IOT issues and concerns, main challenge solutions and finally concludes the study.

Intelligent gadgets enable the general existence of different objects, communicate and cooperate via distinct management systems – the Internet of Things (IoT). IoT, initially launched in 2008-2009, links billions of devices worldwide to various network infrastructure, including the Internet. IoT seeks to combine various conventional and next-generation network technology to operate in a single infrastructure concurrently and to enable various ubiquitous applications. IoT nodes are more diverse compared to others, like WSNs, since they are widely used in many applications and are a major component of cyber-physical systems (CPS).

Many IoT networks are ad-hoc, following the same pattern as WSNs, for instance the Internet of Vehicles, of data transfer to the Internet. IoT nodes interact as an overlay network in such networks, e.g. ZigBee, over an existing ad-hoc network protocol. The fundamental building blocks of such IoT networks are typically WSNs in which sensors connect, interact and exchange data on a huge scale along with a large number of ordinary items. In addition, IoT nodes in these networks are able to interact ad-hoc, owing to the capability of device-to-device (D2D) communication in networks like cellular networks, Wi-Fi and Bluetooth. This makes it possible to communicate more effectively with the co-located IoT nodes and reduce overhead network. In addition, there are many IoT apps running on ad hoc and MANET networks, such as healthcare, intelligence cities, vehicle networks, military applications and smart agriculture [2]. In ad hoc IoT networks, topology management is essential for effective and scalable network administration as well as the applications that are deployed via these networks. Clustering has been presented as the most common topology management method in ad hoc networks like WSNs. Clustering methods split the network into node groups and distribute network functions among group members for enhancing efficiency in, for example, data collection and transmission, resource management and QoS support. For WSN topology management, a number of clustering methods have been suggested, such as LEACH, HEED and TEEN, to mention a few.

Like WSNs, ad-hoc IoT networks may utilise clustering to control topology to satisfy above performance requirements as well as IoT specific problems, such as network scalability. Sharing many of its basic features with WSNs means that ad-hoc IoT networks may possibly use clustering methods without needing to scratch them. The increasing heterogeneity and mobility of IoT nodes, and the integration of IoT into new computing and networking paradigms like edge computing and 5G networks may be difficult. The research community of the IoT thus has a major advantage in undertaking a thorough analysis of current WSN clustering methods and in examining their application to IoT networks. Such survey study may be conducted further by evaluating clustering methods currently utilised in IoT networks. In conducting this comprehensive study, it is essential to establish specific objectives on which elements of current methods should be examined and how the extent of IoT applicability should be considered. Taking into consideration the performance requirements of ad-hoc IoT networks, clusters such as energy consumption reductions, load balancing, connection improvement, etc. should be key to such an investigation [3].

1.1 Intelligent City:

ICTs concentrate on addressing challenges related to the increasing complexity of city complexes, urban infrastructure networks, urban populations and encourage development of future creative "smart cities" initiatives. The 'smart city' idea is meant to be applied in complex metropolitan environments encompassing a range of complex infrastructure systems, behaviours, sophisticated technology, socio-political structures, diverse economy, and so on. The "smart cities" initiatives incorporate sound management techniques for urban components and subsystems such as transport, healthcare, education, power engineering, environmental protection and improvements, etc. In recent years, an extraordinary rise in the number of different kinds of information flows, originating from social networks and the Web, has prompted the development of the new class of information technologies like the Internet of things technology (IoT). Information flows from social and sensory networks may be combined to look for hidden connections and linkages in the "intelligent cities" to expand the variety of the information and services offered. Creative initiatives like Wiki City, City Sense and Google Latitude are being applied in a variety of innovative applications of this kind and in the development of the many social and urban sensor networks. In 'smart cities' initiatives funded financially by the European Community, the benefits of integrated usage of social network information resources and information flows produced by many Internet apps are obvious [4].

In 'intelligent cities' a wide array of activities focused on selecting, transferring, transforming, storing and analysing data flows relating to the state and processes of environmental pollution, meteorological, waste accumulation and utilisation, water supply and other natural resources, heat treatment and processing of large data. At the same time, facts relating to urban life are extracted and transformed from social networks. In particular, the technology of data transmission and selection made up of urban engineering components is based on the usage of wireless sensors integrated in digital industrial and information technology services applications. The integration of data acquired both from physical and social sensors helps to the development of an overview of urban processes, complexes, subsystems and structures. "Smart Cities' Information Systems," based on current information and communication technology, offer strong intellectual assistance both to municipal and urban populations in general [5].

An analysis of the methodological principles of creation of the "smart city" integrated information system of the future should take account of the high degree of complexity of these systems. In general, modern information-technology support systems can be used to support key business processes, to maintain urban engineering infrastructure networks, training and retention of procedures for optimal decisions in municipal management, to efficiently train and operate the municipal social and communications environment in the cities. The structural functional decomposition approach, the main theme of which is to analyse fundamental functions of the separate components of the hyper-complex system, the means and methods that perform these functions, and implement the hyper-complex interaction between elements in a functionally separated part, is one of the most effective tools for these systems analyses.

In this case, the choices are made of such functional complexes as the "sensory" subsystem of the "Smart City," the IoT technology cluster network infrastructure in "smart cities," IT integration with Big Data and cloud computing technological technologies, data storage and space, Data mining and OLAP. Only such a widespread strategy to building a complete information system for the future of the 'intelligent city' may produce substantial creative energy effects from implementation and broad implementation with new characteristics for its people's livelihoods.

1.2 The IoT Overview:

IOT may be defined as a worldwide network of equipment or devices that are physically linked to each other. According to the idea, IOT is simply related things or artefacts that interact with one another to offer intelligent services without human involvement. The Internet reach is extended via IOT. The relationship between electrical devices and computers is currently disguised by the Internet, whereas IOT is developing this for the interconnection of physical things or other products. These are actual goods or objects such as air conditioners, lights, fans, etc. Those things or physical objects are loaded with IT technologies, embedded electronics, embedded networks so that they have an essential processing process connected to each other, and are then moved about as independent internet nodes where nodes connect and exchange data for different transactions. That's mostly how IOT works.

Objects that interact with another object link and operate in the same way. Physical things are sensed or remembered by sensors. The sensors detect various factors such as pressure, temperature, light etc., depending on the sensor being utilised. It is possible to send sensed data and to send data over the network or through the connected device and finally to include the cloud, to transmit data, which are sensed on the basis of the demands, and certain human movements recorded by an actuator [6]. The International Telecommunications Union must specify the 5-layer architecture of the IOT. Researchers proposed dividing IOT, IOT system architecture into three main levels, for instance operating layer, view layer and network layer. The vision layer acquires knowledge about physical things. The network layer is supposed to enable communication in the 3-layer design between the device layer and the vision layer.

It transfers data from the experience layer to the device layer remotely or securely. Be it so, the architecture of the five-layer access gateway layer utilised to communicate between the network layer and the sensitivity layer is involved. It deals with communication structures and objects and also with the IOT environment. The middleware layer further improves the 5-layer design, which provides an interface between equipment and applications which may be increased [7]. The top application layer gives applications or tools to analyse the data received from the rest of the levels. Variables such as privacy & security, networking & connection, device intelligence, scalability, data processing and business modelling must be included throughout the design period of your IOT architecture. The IOT idea should seem like it provides interoperability, respectfulness, portability, adaptability, assessment of quality, protection. SOA is a service-oriented architecture that meets all the features previously described as a superior management method.

1.2.1 Sensing Layer:

RFID and sensor tags wireless or wired or remote systems may share information and contexts between various devices in this tier. Distinctive sensors or markers are utilised in the application for object detection and exchange of information.

1.2.2 Network Layer:

The second layer is often referred to as the transmission layer. The primary function of the transmission layer is to connect everyone. It is also possible to exchange data across the various devices thanks to its availability and is used to transmit data from the sensor to data processing.

1.2.3 Service Layer:

This layer co-ordinates IOT applications and utilities and includes middleware technologies. It involves service APIs, service aggregation, maintenance and service research. This layer also creates any problems with service location, such as the web index, data interchange, contact and data processing.

1.2.4 Layer of Interface:

Users may use this layer to interface with the IOT. Just as IOT is interconnected with everything, it provides many connection options such as machine to entity, machine to machine, machine to application, etc. This coating has a significant impact on the IOT's SOA in these directions. It is generally recognised that different devices are linked to the IOT and are probably made by the particular agency so that they do not conform with comparable specifications or protocols. In this scenario, there may be a difficulty with exchanging information and communicating with various devices. This layer deals with such problems.

1.3 IoT Challenges:

1.3.1 Standardization:

In the last ten years, the ISO is a "International Standardization Organization" which has established that standards are important for the economic and organisational promotion of any business using technology development. It focuses on policies, efficiency and protection that are ecologically sustainable. Due to the employment of conflicting management and development methods, information regarding potential risks is dispersed among users. In the IOT assessment, requirements are the main barriers. Further difficulties are related to the lack of standardisation of IOT goods, such as improvements in interoperability, network consequences and stability. Standardizing IOT devices, design and artefacts are thus essential aspects for the implementation of IOT architectures [8].

1.3.2 Security and Privacy:

Confidentiality and privacy are an important part of the IOT process. For example, it is essential to secure various IOT network activities for storage, personal, data processing and transit operations. Principle 3's security objectives are secrecy, honesty and verification to ensure universal privacy and safety. It should be utilised in all levels of IOT architecture such as middleware layer, sensor layer, device layer, networking layer, and IOT protection.

As a consequence, it is essential for the protection of IOT architecture to be improved and for various privacy and safety frameworks to be developed to address problems of privacy and safety. Authentication is a key element of the IOT ecosystem that has to be modified in order to be completely authenticated for each IOT layer implementation. Authentication enables IOT devices to safeguard the contact system identity to secure the flow of data between various devices [9].

There are thus a few potential attacks due to inability to provide an accurate and acceptable authentication mechanism at any tier of the IOT architecture. Confidentiality is also permitted for secure exchange of communications between users on the network. Encryption techniques or control mechanisms have to be enforced in order to guarantee secrecy. The secrecy and anonymity of the information must guarantee throughout the transmission process that, in any case, the information cannot be changed. Data injection may alter the whole data during the network message exchange.

1.3.3 Consumption of Energy:

The usage of IOT systems in contemporary times increases every day, increasing every day's energy consumption and emitting enormous carbon dioxide into the environment. The energy required to recharge IOT computers, sensors, data processing, gateways, IOT entry points from various IOT infrastructure sensors will be important areas for the possible use of energy. It is also essential in the design of self-sustainable and energy-efficient gadgets, which do not need to recharge the battery until it is dispersed following mobilisation of objects as a battery replacement [10].

2. DISCUSSION

An effective and dependable intelligent infrastructure is the key requirement for the implementation of future intelligent city applications and systems. In this type of infrastructure various basic infrastructures such as (e) water supply systems, (ii) electricity grids and (iii) road, tram and metro transport infrastructure, together with information technologies, distributed intelligent sensing systems, and communication networks, are efficiently and reliably integrated. Another notable use is intelligent healthcare, which may enhance patient quality and healthcare via, for example, better and more rapid diagnosis, better treatment of patients, and increased operational efficiency. Recent advances in the field of control systems combined with contemporary Information and Communication Technology (ICTs) are the primary drivers of the fourth industrial revolution in production settings. This tendency may lead to a dramatic shift in industrial processes in the next decades. A wide-ranging penetration of Machine-to-Machine (M2M) communication and IoT will remove the conventional frontiers between the industrial and communications industries. Thus the major components of a successful and ubiquitous IoT are a large number of sensors, actuators, and many other intelligent devices linked with each other via an omnipresent, high-performance and highly dependable communication network. Optimal combination and integration with intelligent and efficient data collection and processing of these devices is a crucial element in the implementation of integrated and smart systems and infrastructures.

Four stages may split industrial revolutions. New sources of energy were found to operate the machines during the first revolution. Mass coal mining and the creation of steam power plants were important milestones of progress in this era. The second revolution of mass manufacture and generation of energy was a time of fast industrial growth characterised by large-scale manufacturing of iron and steel. Many big factories with their assembly lines were built and new companies started during this period. In the third revolution computer was introduced and communication technologies were first generated, e.g. telephone systems, which allowed the automation of supply chains. The fourth industrial revolution will be empowered by a broad range of contemporary technology, such as communications systems (e.g. 5G), intelligent robots and the Internet of Things. IoT links a variety of devices, people, data and processes, enabling them to interact effortlessly with one other. Thus, IoT may assist to improve the quantification and measurement of various processes by collecting and processing huge amounts of data. IoT may possibly improve the quality of life in many fields, including medical services, smart cities, construction, agriculture, water and the energy sector. This is made possible by increasing automatic decision-making in real time and by offering tools to optimise such choices.

3. CONCLUSION

IOT is an Internet of Things that is a framework or infrastructure for interconnected mechanical machinery, objects, computer equipment, animals or humans, digital machinery that has single identification devices and the ability to transmit information through a network without any necessary contact between human beings or computers. IOT compiles a broad range of objects present in everyday life and encourages them to communicate and make life more intelligent and easy. IOT is the basic infrastructure providing services such as smart communities, health care, robotics, intelligent schools, etc. In the present scenario. Although it currently provides many benefits in various fields, many sectors still have issues with data protection and security, accessibility, scalability, etc. Different businesses manufacture various sorts of computers, cameras, sensors, etc. using various protocol types and different types of technologies. Manufacturing low-standard and low-rate systems creates concerns related to interoperability, security, scalability, safety, energy use, etc. The growth rate of linked equipment increases the consumption of energy or electricity, which impacts the environment considerably. These dangers also offer the way for other researchers to overcome difficulties to build clever and easier lifestyles. It highlighted the many issues and obstacles that need to be concentrated in the IOT.

REFERENCES

[1] P. O. Skobelev and S. Y. Borovik, "On The Way From Industry 4.0 To Industry 5.0: From Digital Manufacturing To Digital Society," *Int. Sci. J. "Industry 4.0,"* 2017.

[2] P. O. SKobelev and S. Y. Borovik, "On the Way From Industry 4 . 0 To Industry 5. 0," *Int. Sci. J. "Industry 4.0,"* 2017.

[3] D. Usha and M. Bobby, "Privacy Issues In Smart Home Devices Using Internet Of Things – A Survey.," *Int. J. Adv. Res.*, 2018, doi: 10.21474/ijar01/7839.

[4] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*. 2017, doi: 10.1109/ACCESS.2017.2779844.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, 2013, doi: 10.1016/j.future.2013.01.010.

[6] A. H. Alavi, P. Jiao, W. G. Buttlar, and N. Lajnef, "Internet of Things-enabled smart cities: State-of-the-art and future trends," *Meas. J. Int. Meas. Confed.*, 2018, doi: 10.1016/j.measurement.2018.07.067.

[7] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sens. J.*, 2016, doi: 10.1109/JSEN.2015.2502401.

[8] S. V. S. V. Prabhu Deva Kumar and S. Akashe, "Implementation of GSM Based Security System with IOT Applications," *Int. J. Comput. Netw. Inf. Secur.*, 2017, doi: 10.5815/ijcnis.2017.06.02.

[9] P. Bhagat and S. Sharma, "Smart AC Power Management," *Int. J. Trend Sci. Res. Dev.*, 2018, doi: 10.31142/ijtsrd18376.

[10] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," 2018, doi: 10.1016/j.procs.2018.05.140.