SUSHANT UNIVERSITY ORGANIZED INTERNATIONAL CONFERENCE ON
"ADVANCES IN MULTIDISCIPLINARY RESEARCH AND INNVOATION" ICAMRI-2023
ON 28-29TH OCTOBER 2023
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Introduction to IOT and Its Technologies

Ms. Ruchy Jain, School of Engineering &Technology, Sushant University, Gurugram, India
ruchy.design@gmail.com
Dr. Koshalpreet Kaur,School of Design, Sushant University, Gurugram, India
koshalpreetkaur@sushantuniversit y.edu.in
Dr. Bindu Thakral, School of Engineering &Technology, Sushant University,Gurugram, India
binduthakral@sushantuniversity.e du.in

ABSTRACT

The term "Internet of Things" (IoT) describes how different physical objects and gadgets are connected online. It is impossible for anyone to ignore the Internet, a revolutionary creation that is continually developing into new technology and apps. The Internet of Things (IoT) looks to the future and promises a significant transition to machine-machine (M2M) communication. The present modalities of communication are either human- human or human-device. In 1999, Kevin Ashton first suggested the term "Internet of Things." Basic IoT concepts are illustrated in the section below. It covers the various IoT levels and some of the fundamental concepts associated with it. In essence, it is an augmentation of Internet services. The IoT architecture is also presented in the section below which outlines the IOT's six layered design and highlights the major difficulties that surround it. In an IoT context, a system is referred to as a smart- home when everyday household appliances are connected to the internet. IOT enabling technologies are also covered in detail in the section below. It is impossible for anyone to ignore the Internet, a revolutionary creation that is continually developing into new technology and apps. IoT is more than simply a bold vision for the future. It has already begun to take effect and affects more than just technical advancement.

Keywords: Internet of things (IOT), RFID, WSN, Cloud computing, IOT technologies, IOT architecture, Networking technologies, Nano technologies,Micro-electro-magnetic system technologies,Optical technologies.

1. Introduction

Due to advancements in wireless technology, the phrase "Internet of Things" has been around for a few years and is currently receiving greater attention. The idea of a network of smart devices was initially suggested in 1982, and the first internet-connected appliance was a customised Coke machine at Carnegie Mellon University that could report its inventory and if freshly filled coke were cold [2]. Kevin Ashton, a British technology pioneer who was born in 1968, is credited with coining the phrase "the Internet of Things" to define a system that connects the Internet to the real world by way of pervasive sensors. The network of physical objects known as the Internet of Things (IoT) includes tools, equipment, electronics, circuitry, software, sensors, and network connectivity in buildings, vehicles, and other objects. This technology allows these objects to gather and share data. In order to more directly integrate the actual world into computer-based systems, the Internet of Things (IoT) can help boost efficiency and accuracy and it enables items to be sensed and controlled remotely through the existing network infrastructure. The fusion of diverse technologies is the key component of the Internet of Things (IoT). The term "Internet of Things" (IoT) refers to the process of linking all objects to the internet. The fundamental purpose of the Internet of Things is to enable autonomous exchange of useful information between invisibly embedded different uniquely identifiable real-world devices around us. This is accomplished with the aid of cutting-edge technologies like Radio-Frequency Identification (RFID) and Wireless Sensor Networks (WSNs), which are sensed by the sensor devices and then processed for decision-making, an automated action is carried out. The paper is organised as follows.

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Section 2 discusses the technologies that IOT is composed of Section 3 major key issues and challenges & section 4 concludes the paper.

ARCHITECTURE

In order to handle a network as large as the Internet of Things, which is expected to have more than 25 billion connected devices by 2020 [14], It is necessary to develop a new open architecture that might use open protocols to serve existing network applications while also addressing a number of security and Quality of Service (QoS) challenges. The Internet of Things is expected to have more than
25 billion connected devices by 2020 [36]. IoT adoption is unlikely to be widespread without a suitable promise of privacy [34]. Thus, the protection of data and user privacy are major IoT challenges.

Division of IOT Architecture as shown in the Fig. I. The six skins of IoT are described below:

1.1 Coding skin

IOT is built on a coding layer that gives objects of interest identification. Each object in this layer has a distinct ID, making it simple to identify the objects.

1.2 Perception skin

Sensors perceive the environment and acquire data about it.

1.3 Transport skin

uses networks including WIFI, 3G, LAN, Bluetooth, RFID, and NFC to transfer sensor data between different skin types.

1.4 Processing skin

massive volumes of data are stored, processed, and analysed. Employs databases, cloud computing & big data processing modules.

1.5 Application skin

accountable for providing the user with application-specific services.

1.6 Business skin

manages the IOT system as a whole, including its applications, businesses, and business models, and user's privacy.

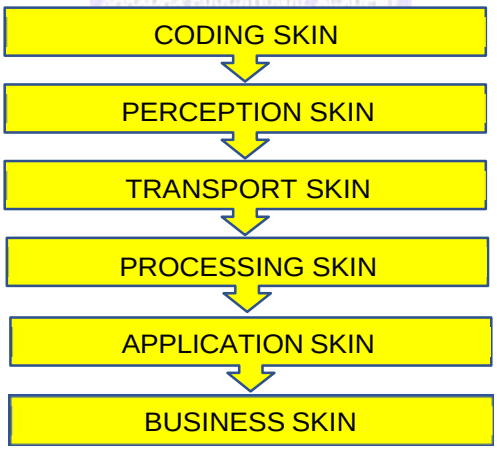

Fig. I Six skins of IOT Architecture

Author's own compilation

2. TECHNOLOGIES

The creation of a global computing system, where digital objects are able to be individually identified, think, and communicate to other objects in order to gather information from which actions that are automated are taken, necessitates an amalgamation of new and efficient technologies, which is only made possible by the

combination of various technologies that enable the identification and communication of the objects [3]. This section covers the pertinent technologies that can aid in the widespread growth of the Internet of Things.

3.1 Wireless Sensor Network (WSN): A WSN is a bi-directional, multiple-hop wireless sensor network made up of nodes dispersed throughout a sensor field, each of which is linked to a sensor that can collect information about an object, such as its temperature, humidity, speed, etc., and communicate it to processing machinery [5]. The sensing nodes communicate across many hops. With an antenna, a microcontroller, and an interface circuit, any sensor is a transceiver. that serve as the sensors' communication, actuation, and sensing units, respectively. Each sensor also has a power source that may be a battery or a gadget that captures energy [6]. However, [7] has proposed a second memory unit for data storage, which may also be a component of the sensing node.

Mobile Sensors When network technology and RFID technology are integrated, the potential for even more smart devices is increased, and several solutions have been suggested [5]. The Intel Research Labs' Wireless Identification Sensing Platform (WISP) serves as an illustration of a solution [8]. With built-in light, temperature, and other sensors, WISP is a passive wireless sensor network [9]. Both WSN and RFID Sensor Networks have benefits, but WSNs have a much wider range and peer-to-peer communication, whereas RFID Sensor Networks have a small range and asymmetric communication. The IEEE 802.15.4 standard [5], which describes the physical and MAC layers of LR- WPANs (Low-Rate Wireless Personal Area Networks), is also the foundation for the majority of WSNs.[10]

3.2 Radio Frequency Identification (RFID): The main technique for making the objects individually identifiable is RFID. It may be integrated into any object because to its small size and low cost [1]. Depending on the application, it is a transmitter microchip that resembles an adhesive sticker and can be either active or passive [5]. Because they are powered by a battery, active tags are always on and continuously send out data signals, whereas passive tags only turn on when they are triggered. Although active tags are more expensive than passive tags, they have many more practical uses [7]. The RFID system consists of readers and related RFID tags that, when activated by the production of any suitable signal, transmit information about the object, including its identification, location, and other details [2]. The radio frequencies used to transmit the produced object-related data signals are subsequently handed on to the processors for data analysis.

RFID frequencies are classified into four different frequency bands [11], which are listed below, in regard to the type of application:

(1) Low frequency (135 KHz or less)
(2) High Frequency (13.56MHz)
(3) Ultra-High Frequency (862MHz 928MHz)
(4) Microwave Frequency (2.4G, 5.80)

While RFID is more effective than Bar Code, it is another identification technology that accomplishes the same goal because of a number of its advantages. Unlike RFID, which uses radio technology and doesn't require the reader to be physically in its line of sight, bar codes are optical technologies that require the reader to be positioned in front of them in order to work. Additionally, unlike bar codes, an RFID can operate as an actuator to start various events and even perform modifications.

Networking Technologies: We require a quick and efficient network to manage a huge number of potential devices because these technologies are crucial to the success of IoT as they are in charge of connecting the things. As we move into the modern era of ubiquitous computing, mobile traffic will no longer be predictable, necessitating the need

for a fifth-generation wireless technology that is extremely quick and effective that might provide a lot more bandwidth [12]. Currently, we commonly use 3G, 4G, etc. in the case of wide-area transmission networks. Mobile traffic, on the other hand, is well known to be very predictable since it simply needs to carry out routine operations like making calls, sending texts, etc. Similarly, we employ technologies like Bluetooth, Wi-Fi etc. for ashort-range communication network.

3.3 Nano Technologies: The connected objects are made smaller and better thanks to this technology. By facilitating the creation of nanometre-scale devices that can function as a sensor and an actuator just like a regular device, it can reduce the consumption of a system. Such a nano gadget is constructed from nano components, and the network it creates—known as the Internet of Nano-Things— defines a new networking paradigm. [12]

3.4 Cloud Computing: By 2020, millions of devices are expected, and the cloud seems to be the only technology that can support them capable of efficiently analysing and storing all the data. It is a sort of intelligent computing in which numerous servers are brought together on a single cloud platform to enable resource sharing that is accessible from anywhere at any time [14]. The most crucial component of IoT is cloud computing, which not only consolidates servers but also processes data with improved processing power, analyses valuable information gleaned from sensors, and even offers adequate storage [15] refer to fig. II. But the actual potential of this technology has yet to be fully realised. Since IoT will be entirely dependent on cloud computing, research is being done to see how the integration of cloud computing with smart devices that may use millions of sensors can have significant advantages and support the growth of the Internet of Things on a very large scale.

Fig. II A Typical Cloud computing scenario

3.5 Micro-Electro-Mechanical Systems (MEMS) Technologies: MEMS and Nano technologies work together to improve the IoT's communication system while also providing other benefits, including as smaller sensors and actuators, a larger frequency range, integrated ubiquitous computer devices, and [16].

3.6 Optical Technologies: optical technologies are developing quickly, including Li-Fi and Cisco's BiDi optical technology and may represent a significant step forward for the Internet of Things. Li-Fi, a revolutionary Visible Light Communication (VLC) technology, will offer excellent connectivity and increased bandwidth for the IoT-connected objects. Similar to the previous example, Bi- Directional (BiDi) technology provides a 40G ethernet for huge data from several IoT devices [17].

3.7 Near Field Communication (NFC): It is a collection of communication protocols that enables two electronic devices to establish connection by being within 4 cm (2 inches) of one another [18]. One of the devices is typically a portable device like a smartphone. NFC, or near field communication, is a method of contactless communication between gadgets like smartphones or tablets. Without having to touch the devices or take additional steps to establish a connection, contactless communication

enables a user to wave their smartphone over an NFC-compatible device to convey information. Through the NFC Forum, near field communication upholds compatibility between various wireless communication techniques like Bluetooth and other NFC standards, including FeliCa, which is well- known in Japan. The forum, which was established in 2004 by Sony, Nokia, and Philips, imposes rigid requirements on manufacturers for creating NFC- compatible products. By doing this, NFC is guaranteed to be safe and simple to use across all generations of the technology. The development of NFC as a well-liked payment and data transfer technique depends on compatibility. It must be able to engage with various NFC broadcasts and communicate with other wireless technologies.

The NFC system enables a device—also referred to as a reader, interrogator, or active device—to generate a radio frequency current that communicates with another NFC-compatible device or a tiny NFC tag storing the data the reader needs. The NFC tag in smart posters is an example of a passive gadget that stores information and communicates with the reader but does not actively read other devices. NFC also allows for peer-to-peer communication between two active devices. As a result, data can be sent and received between the two devices. Each full NFC gadget has three operating modes.

a. NFC card emulation-- permits smart cards to behave like NFC-capable devices, such as smartphones, allowing users to conduct transactions like payment or ticketing.

b. NFC reader/writer-- permits information stored on cheap NFC tags placed in labels or smart posters to be read by devices with NFC capability.

c. NFC peer-to-peer-- enables the ad hoc communication between two NFC-capable devices to exchange information.

3.8 Data Visualization: A user needs to be able to interact with an IoT-based system effectively, hence appropriate data visualisation techniques must be used. IoT-based applications have undoubtedly benefited from advancements in touch screen, display, and smart phone technologies. Data visualisation for end users has become more dynamic and effective thanks to 2D and 3D technology. It is difficult to extract useful information from raw data. This includes event detection as well as the visualisation of the related unprocessed and modelled data, with information displayed in accordance with user requirements.

3. MAJORKEY ISSUES AND CHALLENGES

The Internet of Things (IoT) has a significant impact on all facets of modern life, and the various technologies used to transfer data between embedded devices have complicated the situation and created new problems. In the sophisticated smart technology society, these problems also provide a difficulty for IoT developers. Challenges and the need for advanced IoT systems are expanding along with technology. IoT developers must therefore consider potential problems as they arise and offer solutions.

Security and privacy issues

Due to numerous threats, cyberattacks, hazards, and vulnerabilities in the IoT, security and privacy are among the most crucial and difficult challenges [19]. Insufficient authorisation and authentication, unreliable software, unreliable firmware, unreliable web interfaces, and inadequate transport layer encryption are the problems that lead to device level privacy [21]. Concerns over security and privacy are crucial factors to consider while developing confidence in IoT systems with regard to numerous elements [20]. To stop security risks and attacks, security procedures must be built into the IoT architecture at every layer [22]. To secure the security and privacy of IoT-based systems, a number of protocols have been created and are being deployed effectively on every tier of communication channels [23, 24]. Secure Socket Layer (SSL) and Datagram Transport

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Layer Security (DTLS) are two cryptographic protocols that are implemented between the transport and application layers in order to provide security solutions in various IoT systems [23]. To guarantee the security of inter-IoT device connection, many IoT applications call for alternative approaches. Additionally, the IoT system is more susceptible to security threats if communication occurs utilising wireless technology. Therefore, specific techniques should be used to identify malicious behaviour and to promote self- healing or recovery. Contrarily, privacy is still another crucial issue that users must consider in order to feel secure and at ease when utilising IoT technologies. As a result, maintaining authorisation and authentication over a secure network is necessary to establish communication between parties who can be trusted [27]. The various privacy regulations for various objects communicating within the IoT system is another problem. Therefore, before sending data to another object in an Internet of Things system, each object should be able to check their privacy policies.

Standards and interoperability problems

The ability to communicate information between various IoT systems and devices is known as interoperability. This information transmission is not dependent on the installed software and hardware. The diverse nature of the various technologies and solutions utilised for IoT development gives rise to the interoperability issue. The four interoperability layers are organisational, technological, semantic, and syntactic [28]. In order to increase interoperability and assure communication between various items in a heterogeneous environment, IoT systems offer a variety of functionalities. Additionally, different IoT platforms can be combined based on their characteristics to offer different IoT users solutions [29]. Researchers approved a number of methods, also known as interoperability management approaches, because they viewed interoperability as a crucial issue [30]. These solutions could be built on the basis of adapters or gateways, virtual networks or overlays, service-oriented architecture, etc. There are still some interoperability difficulties that could be the subject of future research, despite the fact that interoperability handling mechanisms reduce some of the burden on IoT systems [30].

Quality of Service (QoS)

Quality of service, or QoS, is another essential component of the Internet of Things. A metric for evaluating the quality, efficacy, and functionality of IoT systems, architecture, and devices is known as QoS [30]. For Internet of Things applications, reliability, affordability, energy use, security, availability, and service time are essential and required Quality of Service criteria [31].

CONCLUSION

The idea of the Internet of Things is rapidly and inescapably expanding on a very large scale. By incorporating intelligence into the things around us, every element of our life will be impacted by this new networking paradigm, from automated houses to smart health and environment monitoring. Researchers and developers from all around the world are interested in recent developments in IoT. IoT researchers and developers are collaborating to advance technology on a big scale and benefit society as much as feasible. However, advancements are only attainable if we take into account the different problems and shortfalls in the current technical approaches. In this research paper, we discussed a number of major key issues and challenges that IoT developers must consider while creating a better model. We emphasised a number of enabling technologies. The next Internet trend has been the Internet of Things. Everything in the world is becoming intelligent. There is a lot of room for IoT research. In the future years, there will be a huge influx of new technology, elevating our level of a smart world. The IoT has a very

promising future. Everything would be connected, resulting in a better way of living, from our bills to our vehicles.

REFERENCES

1 Wang Chen," AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS," in Cloud Computing and Intelligent Systems (CCIS), 2012, pp. 1046, 104

2 H. Zhang, L. Zhu," Internet of Things: Key technology, architecture and challenging problems", in Computer Science and Automation Engineering (CSAE), 2011, Volume: 4, pp. 507-512

3 Benjamin Khoo," RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in Internet of Things (iThings/CPSCom), 2011, pp. 709-712

4 "The "Only" Coke Machine on the Internet". Carnegie Mellon University. Retrieved 10 November 2014.

5 L.Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey," in Computer Networks - Science Dir

6 Sohraby, K., Minoli, D., Znati, T." Wireless sensor networks: technology, protocols, and applications", John Wiley and Sons, 2007 ISBN 978-0-471-74300-2, pp. 15-18

7 Guicheng Shen and Bingwu Liu," The visions, technologies, applications and security issues of Internet of Things," in E -Business and E - Government (ICEE), 2011, pp. 1-4

8 "WISP" by Intel Labs; It can be accessed at: http://wisp.wikispaces.com

9 E. M. Tapia, S. S. Intille, and K. Larson," Portable wireless sensors for object usage sensing in the home: Challenges and practicalities," in Proceedings of the European Ambient Intelligence Conference. vol. LNCS 4794 Berlin Heidelberg: Springer-Verlag 2007

10 IEEE 802.15 WPAN Task Group 4. It can be accessed at: http://www.ieee802.org/15/pub/TG4.html

11 L.G. Guo, Y.R. Huang, J. Cai, L.G. QU," Investigation of Architecture, Key Technology and Application Strategy for the Internet of Things," in Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011, Volume: 2, pp. 1196-1199.

12 O. Vermesan, P.Friess," Internet of Things? From Research and Innovation to Market Deployment," River Publishers, pp. 74-75.

13 Kyildiz and J. Jornet," THE INTERNET OF NANOTHINGS," IEEE Wireless Communications, Volume: 17 Issue: 6, 2010, pp. 58-63

14 Gartner, Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717B.B.P. Rao, P. Saluia, N. Sharma, A. Mittal, S.V. Sharma," Cloud computing for Internet of Things & sensing based applications," in Sensing Technology (ICST), 2012 Sixth International Conference, IE

15 Xiaohui," Study on Security Problems and Key Technologies of The Internet of Things," Computational and Information Sciences (ICCIS), 2013, pp. 407-410

16 I.akyildiz and J. Jornet," THE INTERNET OF NANOTHINGS," IEEE Wireless Communications, Volume: 17 Issue: 6, 2010, pp. 58

17 " Cisco 40 Gigabit Module".
It can be accessed at: http://www.cisco.com/c/en/us/products/interfacesmodules/40-gigabit-modules/index.html

18 Ortiz, C. Enrique (June 2006). "An Introduction to Near-Field Communication and the Contactless Communication API". Retrieved 2008-10-24.

19 Babovic ZB, Protic V, Milutinovic V. Web performance evaluation for internet of things applications. IEEE Access. 2016; 4:6974–92.

20 Xu LD, He W, Li S. Internet of things in industries: a survey. IEEE Trans Ind Inf. 2014;10(4):2233–43 Internet of Things research study: Hewlett Packard Enterprise Report. 2015. http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050. WPoNH6KxWUk

21 Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. J Netw Comput Appl. 2014; 42:120–34

22 Dierks T, Allen C. The TLS protocol version 1.0, IETF RFC, 2246; 1999. https://www.ietf.org/rfc/rfc2246.tx

23 Pei M, Cook N, Yoo M, Atyeo A, Tschofenig H. The open trust protocol (OTrP). IETF 2016. https://tools.ietf.org/html/ draft-pei-opentrustprotocol-00

24 Roman R, Najera P, Lopez J. Securing the internet of things. Computer. 2011;44(9):51–8.

25 Van-der-Veer H, Wiles A. Achieving technical, interoperability-the ETSI approach, ETSI White Paper No. 3. 2008.http://www.etsi.org/images/fles/ETSIWhitePapers/IOP%20whitepaper%20Edition%203 %20fnal.pdf

26 Colacovic A, Hadzialic M. Internet of things (IoT): a review of enabling technologies, challenges and open research issues. Comput Netw. 2018; 144:17–39

27 Noura M, Atiquazzaman M, Gaedke M. Interoperability in internet of things infrastructure: classifcation, challenges and future work. In: Third international conference, IoTaaS 2017, Taichung, Taiwan. 20–22 September 2017.

28 Temglit N, Chibani A, Djouani K, Nacer MA. A distributed agent-based approach for optimal QoS selection in web of object choreography. IEEE Syst J. 2018;12(2):1655–66.

29 Huo L, Wang Z. Service composition instantiation based on cross-modified artificial Bee Colony algorithm. Chin Common. 2016;13(10):233–44.

30 Jian An, Xiao-Lin Gui, Xin He, "Study on the Architecture and Key Technologies for Internet of Things," in Advances in Biomedical Engineering, Vol.11, IERI-2012, pp. 329-335

31 "From the ARPANET to the Internet" by Ronda Hauben - TCP Digest (UUCP). Retrieved 2007-07-05 It can be accessed at: http://www.columbia.edu/ rh120/other/tcpdigest paper.txt

32 Lan Li, "Study of Security Architecture in the Internet of Things," in Measurement, Information and Control (MIC), 2012, Volume: 1, pp. 374-37