iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** X **Month of publication:** October 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.47047

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue X Oct 2022- Available at www.ijraset.com*

# IOT Architecture, Challenges and Opportunities

Deversh Khandelwal[1], Manjot kaur Bhatia[2]
[1]*MCA Student,* [2]*Professor, Jagan Institute of Management Studies*

***Abstract:*** ***The Internet of Things, as defined by the Internet itself, is the connection of embedded computing devices embedded differently within the existing infrastructure. According to IoT, soon our planet will contain the largest number of devices connected to the Internet. This paper is a discussion of the trending term 'Internet of Things' challenges and opportunities, as well as the formation of IoT, which describes widely used technologies such as M2M communications, cloud computing, IPv6, and RFID technologies, thus describing the use of IoT different fields. Finally, there is a brief review of all possible IoT applications.***

***Keywords: Internet of things, M2M, cloud computing, RFID, Machine Learning, IPv6, Automation, SDN, NFV***

## I. INTRODUCTION

IoT is an application that connects you to your tool, or maybe device to system, for smooth get right of entry to tool features. Its scope not best applies to the idea of simplicity but additionally extends to using numerous technologies and devices in order to acquire faster overall performance and a safer environment.[1] The idea of IoT has been around for years, however, there was a fast boom in the variety and forms of gadgets linked and processed. IoT refers to a device in which objects within the physical global use sensors internally or connected to these gadgets, linked to the internet through a wireless and wireless network connection. these sensors can use a spread of neighborhood connections including radio- frequency identity (RFID), near community (NFC), wi-fi fidelity (wi-fi), and Bluetooth. Sensors can also have broadband connectivity such as global telecommunications gadget (GSM), trendy packet radio service (GPRS), third-era (3G) and 4G and 5G cellular communique offerings, and long time evolution (LTE).[5]

## II. ARCHITECTURE OF IOT

It serves the complete purpose of depicting the configuration of the IoT system when into various deployments for different purposes. The different layers of IoT can be discussed as follows.

### *A. Sensors Connectivity Layer*

Sensors are the basic connectivity of the appliance to further layers. They are different according to various uses. Some of the devices of this layer that participate in the IoT are sensors and actuators in smart cities, smart tags on many familiar objects, wearable health monitoring sensors, smartphones, intelligent cars, and smart home appliances.[2]

### *B. Network Layer*

A huge quantity of data will be produced through those sensors and thereafter they require a totally full-size community of wired or wi-fi mediums for transportation. this will be inside the shape of a nearby location network (LAN) which includes Ethernet and wireless connections or a private area community (PAN) inclusive of ZigBee, Bluetooth, and ultra- Wideband (UWB).[4] The problem that arises nowadays is that the IoT is generating completely new types of statistics, with a lot greater common updates of a good deal smaller sizes, on unpredictable schedules and furthermore, in addition, they require a better QoS. modern wi-fi network technology, which includes RFID and wi-fi, may discover a conversation answer in an IPv6-primarily based community, which is likewise generally diagnosed because the maximum sensible answer nowadays.[7] To provide greater efficient performance, the enterprise will circulate towards software-based answers like network features Virtualization (NFV) and software- described Networking (SDN).[6]

### *C. Management Layer*

This residue is chargeable for data evaluation/management and safety monitoring with the aid of encrypting and controlling get right of entry to transmitted data. Cristian Borce (accomplice Professor of pc technology at the New Jersey Institute of the era) in collaboration with the countrywide Institute of Informatics (NII) in Japan, performed studies on a way to use cloud computing era and software-defined networks (SDN) to enhance.[5] powerful and efficient IoT services.

This research brought about the belief that the future of the IoT should evolve over the prevailing net and install a disbursed architectural intelligence novel known as the 3DIA - a "three-dimensional intelligence structure". 3DIA is primarily based on three design concepts:

- Distribution of IoT offerings
- IoT community inspired by means of SDN principles
- IoT full cloud-based totally guide

By using 3DIA, internet gadget devices may be able to utilize dispensed listening to and computer services with cloud aid, which can also address troubles related to availability, provider restrictions, bandwidth, delays, and control.[8]

### *D. Application Layer*

After storing, processing and analyzing data intelligently, this layer delivers the results based on users' requests. As a vast array of data involved, the system integrates distributed computing technologies, such as P2P (Peer to Peer) and cloud computing, which both facilitate intelligent analysis and processing, decision making, and enhance the capacity of information processing in the IoT. Typical applications include monitoring in security, and disaster, as well as intelligent household appliances and vehicle scheduling. The above stated 4 layer architecture is the most suitable structure to cover up all the domains of the IoT system. However, it cannot express the whole features and connotations. It needs to be added and improved with the development of the IoT technologies. Some researchers have already put forward a five-level architecture, including the business layer, application layer, processing layer, transport layer and perception layer. No matter what the changes are, the architectures remain essentially three keywords: perception, transmission and processing.

## III. USE OF IOT IN FUTURE

while gadgets are able to make a selection[figure 1] on the premise of outcomes being acquired from the enter sensors, without a requirement of human intervention then it allows the device to run extra cutting-edge evaluation and take extra complex picks and respond to local desires fast. So let us test some destiny scope of IoT in terms of its software.

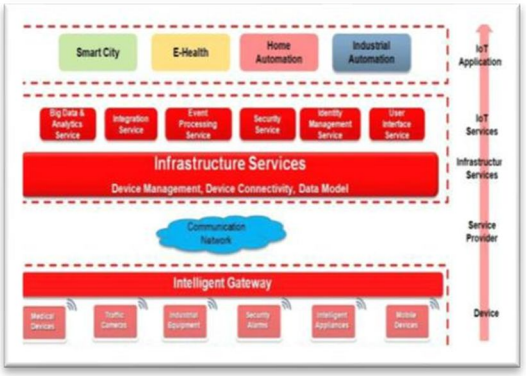



Fig 1: Uses of Internet of Things (IoT)[1]

### *A. Asset Tracking*

Asset monitoring, today eliminated by barcode and the spread of measures, but in the future, will use smart tags, word processing (NFC), and RFID to track worldwide all types of items, collectively. The term geo-tagged is now used by a few agencies to negotiate this beauty of apps.[9] In the future, one may be able to use Google Earth to sing something with the RFID tag. instead, your refrigerator should keep track of your smart groceries smart and tell your mobile app that you are down to something. in case your frozen vegetable bag can have a smart tag, various items and valuables, rings and wallets should also, and can be tracked online and be able to take advantage of packages available on the web.

### *B. Process Manage And Optimization*

When multiple sensors in the system are used for the same purpose of monitoring and providing data so that the process is remotely controlled. This can be as simple as using cameras used to place boxes of various sizes on a conveyor belt so that the label machine can properly label them. This work can be done in real time by sending data to a remote computer, analyzing it, and returning the command to the line for various control measures to improve the process, without human intervention.[10]

*C. Context-Aware Automation*

This section is the most interesting, as it refers to monitoring factors such as environment, interaction between machinery and infrastructure, etc. and having machines that make human-like decisions. Here is an example that can help to illustrate: In a car-collision control system (TCAS), when two planes approach each other in a collision course, the 'machines' on the two planes take off. The system first sends sound warnings to pilots of an aircraft accident, while simultaneously connecting the two aircraft and determining the direction of each flight to avoid a collision. It is thought that if two pilots were warned and controlled to make quick decisions, both would decide to take a risk.[2] There are a lot of new technologies available today and are being developed that would allow cars to interact independently with the central control unit. These smart cars can detect road signs, traffic signals, and route signs and, with the use of GPS and communication link, avoid inconvenient traffic and avoid accidents.

*D. Identity Security*

Based on the identification technology, a person can be identified. Some countries start projects to deploy identity card systems for their citizens. Typically, each citizen has an ID card where a chip is embedded and some private enciphered data are stored [11]. The reading devices are deployed in secure environments, and the reading processing will be operated by a well-trained clerk to ensure the security of the ID card system. But the public security in the IoT leads to some new and urgent requirements which include:

1) *Digital Identities:* A citizen usually has many types of digital identities. Thus, it is very important and urgent to provide a simple, pervasive, and trusted link between citizens and the database in the IoT. After setting up the link, citizens can securely visit the services in the IoT, whereas the government can effectively manage the IoT.
2) *Authentication For Online Services:* Online banking and e-government services are more and more popular in the current Internet society. In the services, the first securityconsideration is to authenticate the user'sidentity, especially to authenticate whether the user is a person in the real world. User authentication can be done using steganography based authentication system proposed by Bhatia[13,15]. Finger based user authentication is possible for online services[14].

*E. Smart Grid*

The smart grid system is an electricity transmission and distribution network that adoptsadvanced wireless sensor nodes as "ears and eyes" to collect detailed information about the transmission and distribution of electricity[figure 2]. Integrated with robust bi-directional communications and distributed computers, the smart grid is a self-adaptive system to counter fluctuating and unstable demands of electricity in order to improve the efficiency, reliability, and safety of power delivery.

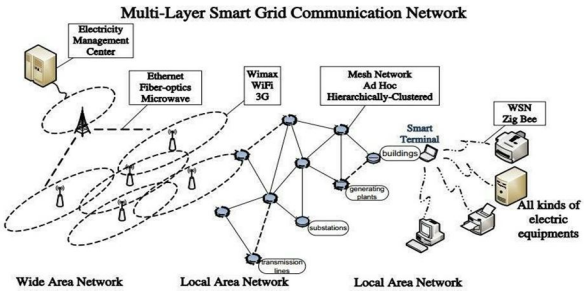



Fig 2: Layers of IoT[12]

## IV. TECHNICAL CHALLENGES OF IoT

1) *Security:* because IoT connects large gadgets together, it provides extended access to malware. Low-priced devices that can be at risk are a major problem of disruption.[6] Additional layers of software programming, middleware integration, APIs, gadget word-to-device exchange, and much more. create more complexity and new security risks.
2) *Consider and Confidentiality:* With remote sensors monitoring the IoT center usage environment, theremay be greater sensitivity to control acceptance and statistical identity.
3) *Complexity, confusion, and Integration Problems:* With a few programs, multiple agreements, and large numbers of APIs, integration of IoT architecture and experimentation will be a task, to say the least. Confusion about changing values is sure to be accepted gradually. The rapid emergence of APIs will consume unexpected development resources in a way to reduce the capabilities of allocation teams to add new intermediate functionality.[4]

4) *Flexible buildings, Protocol Battles, and Competitive levels:* As more and more gamers worry about IoT, there will be ongoing battles as legitimate companies seek to secure the blessings of their ownership properties and open architects trying to set new standards.[6] There may be many changing values based on different needs determined by device quality, electrical requirements, power, and usability.

## V. FINAL THOUGHTS

The IoT is developing very quickly, and we introduce the technical view to the IoT which includes the structure fashions, community, and communication technology, discovery and seek engine technologies, security and privateness technologies, packages, and technical challenges. The pervasiveness of embedded processing is already taking place anywhere around us. At domestic, appliances as mundane as your simple toaster now come with an embedded MCU that now not only sets the darkness of the piece of toast in your choice but additionally adds useful safety to the tool. Your refrigerator has started out speaking to you and preserving song of what you put in it. There are energy-aware HVAC systems that may now generate a report on the interest in yourown home and recommend approaches to reduce your energy intake.[2] The electrification of vehicles has already begun taking place, and in only some years from now, every car will contain >50 percent extra electronics than it did just five years ago. The vehicles of the future will indeed be able to pressure themselves. similar modifications also are occurringin different aspects of our lives … in factories, transportation, school structures, stadiums, and other public venues. Embedded processing is everywhere. Connecting the clever devices (nodes) to the internet has also started occurring, even though at a slower rate.[3] The pieces of the generation puzzle are coming together to accommodate the net of things sooner than the majority count on. simply because the net phenomenon passed off not see you later in the past and stuck like a wildfire, the net of things will touch every issue of our lives in less than a decade.

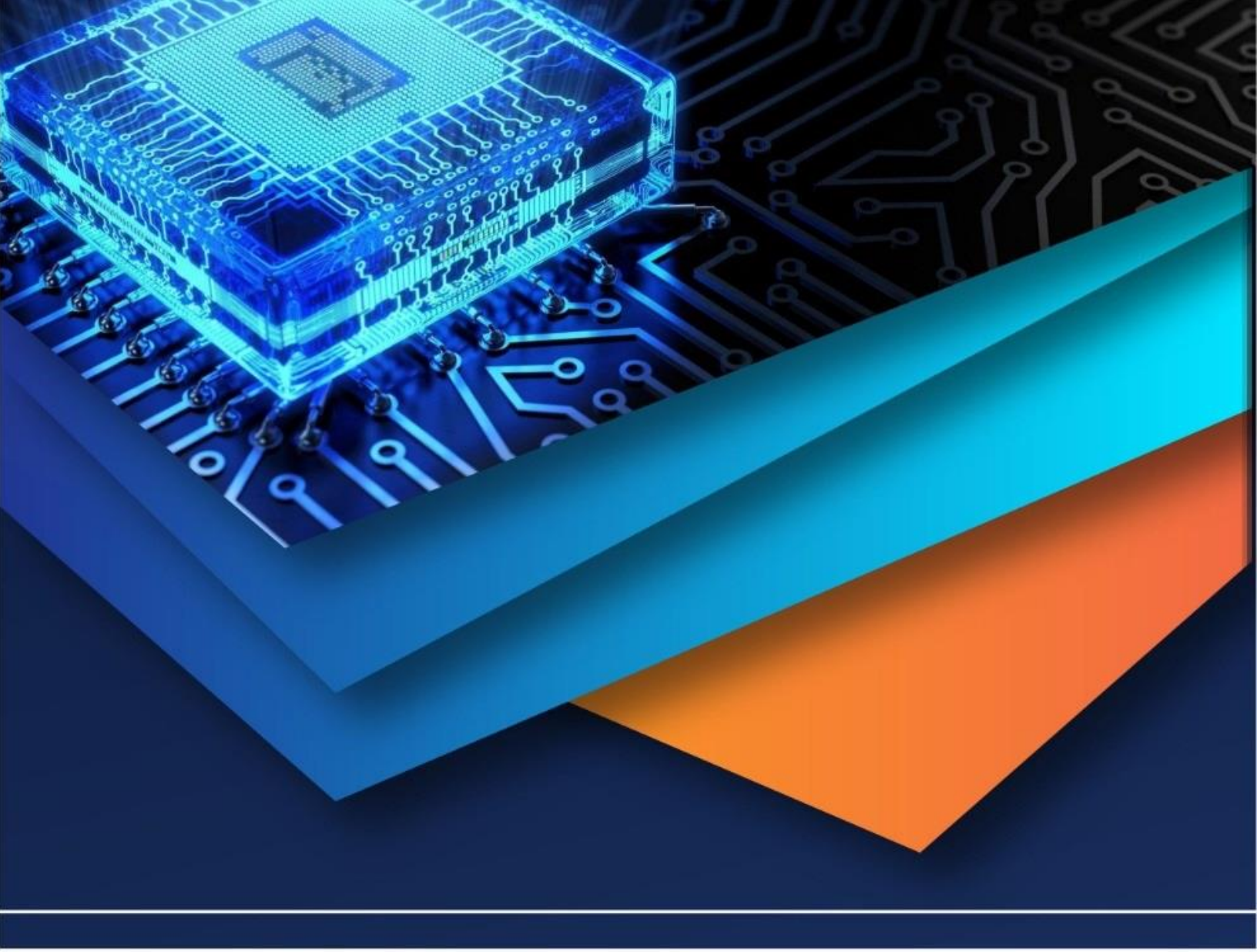
## VI. CONCLUSION

There is a lot of research in many different areas involving IoT. Many different researchers have proposed many different kinds of adaptations to protocols and authentication methods for IoT which makes it very difficult to identify the best solution.

Therefore, there is a grave need for structured guidelines in the form of standardization in order to interconnect all kinds of devices, protocols, applications, etc. Developing standards or solutions need to come with open-source protocols and methods in order to attract wide acceptance and use.By trying to give an understanding of how such a standard should be developed and what requirements are needed, we hope that we have helped layer a foundation for further studies in the area.

## REFERENCES

[1] InternetofThings,2014http://www.itu.int/en/publications/ gs/pages/publications.aspx?parent=SPOLIR.IT2005&me dia=paper#
[2] InternetofThings,2015http://www.rfidjournal.com/article s/view?4986.
[3] Sarfraz Alam, Mohammad M. R. Chowdhury, Josef Noll, 2010 SenaaS:An Event-driven Sensor Virtualization Approach for Internet of Things Cloud, Networked Embedded Systems for Enterprise Applications (NESEA), 2010 IEEE International Conference on, 1-6.
[4] Andras Kalmar, Rolland Vida, Markosz Maliosz, 2013 Context-aware Addressing in the Internet of Things using Bloom Filters, Cog l nfoCom 2013· 4th IEEE I nternational Conference on Cognitive I nfocommun ications' (Dec. 2013) 487 - 492.
[5] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, 2013 Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 1645-1660.
[6] Daoliang Li, Yingyi Chen, Oct. 2010, Computer and Computing Technologies in Agriculture. Springer, 24-31.
[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] Huansheng Ning, Hong Liu, 2012 Cyber-Physical-Social Based Security Architecture for Future Internet of Things, Advances in Internet of Things, 1-7.
[10] 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.
[11] D.Giusto, A.lera, G.Morabito, L.Atzori (Eds.), 2010 Objects Communication Behavior on Multihomed Hybrid Ad Hoc Networks, Springer, 3-11.
[12] Sudip Misra, P. Venkata Krishna, Harshit Agarwal, Anshima Gupta, Mohammed S.Obaidat, 2012 An Adaptive Learning Approach for Fault-Tolerant Routing in Internet of Things. IEEE Wireless Communications and Networking Conference: PHY and Fundamentals, 815 – 819.
[13] Bhatia, M. K. (2020). User authentication in big data. In Soft Computing: Theories and Applications: Proceedings of SoCTA 2018 (pp. 385-393). Springer Singapore.
[14] Bhogal, S. K., Singh, R. K., Talwar, H., & Bhatia, M. K. (2021). Biometric ATM Iris Recognition with Fingerprint Scanning and GSM Module. NOVYI MIR, 6(8), 81-87.
[15] Bhatia, M., Muttoo, S. K., & Bhatia, M. P. S. (2013). Secure group communication with hidden group key. Information Security Journal: A Global Perspective, 22(1), 21-34.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY