International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 2, Mar-Apr-2022, ISSN (Online): 2395-566X

IOT: Prime Challenges, Problems and Analysis using New Technologies

K. Rajkumar, G. Sai Keerthi, N.Pooja
Department of Electronics and Communication,
JNTUH, Hyderabad, Telangana, India
rajkumarkummari17@gmail.com, keerthigudikandula12@gmail.com, pooja.nakka1@gmail.com

Abstract- Internet of things is best domain for sharing and for communicate the data to real world. Now a day's many things are connected with each other using different mediums and produce information various formats and offers different service. IoT brilliance in internally connected objects for communicate, giving information to others and making decisions and to provide service service as per our requirement. The network protocols and architecture use things, information produced by the things leads to several issues such as policy issue, security issue, complexity and standardization. This research gives the idea about the different challenges of internet of things and various issues, as it leads to technologies which are associated for internet of things and provides the solutions to the issues.

Keywords- IoT, IoT architecture, network layers, standardization, sensors, security and privacy, energy consumption, Identity management, Interoperability, scalability, Blockchain, Bigdata.

I. INTRODUCTION

Small changes in technology will change people`s lives and lifestyles. When the invention of the telephone was completed, human life changed. New technologies are used to make human life easier and more comfortable today.

Many popular IoT Internet during this period. Kevin Ashton introduced the "Internet" in 1998. The AutoID Center 2001 wills the implement the IoT vision in AutoID. Today you can see the use of IoT in everyday life. Wearables, example, can tell you your health by analyzing the distance traveled by a person.

B. By heart rate or step count analysis. In the near future, we plan to use phones, cameras, wearables, and special sensors to diagnose health problems. Like that. Therefore, healthcare services will be available 24 hours a day, 7 days a week, anywhere in the world. The name of the technology itself indicates that it is used to interconnect different things in order to provide a higher level of service to society and the economy.

As a result, IoT provides platforms for connecting different devices as well as Calculate anytime and anywhere. IoT offers different types of applications such as smart homes, smart city, and smart transport, smart parking can be used in various fields such as home automation, medicine, agriculture, transportation, and factory. IoT brings many benefits, making people's lives easier and more convenient, but as the number of supplied devices increases, this is the number of issues.

The increase in the percentage of related devices leads to energy consumption such as, CO2 emissions, network complexity, connectivity issues, shared data security, confidentiality, and interoperability of connected gadgets.

Standardization of different devices in different companies, as well as increased communication protocol used. B. Damura contains manuals for many researchers to address it. This document is divided into several sections; part 2 describes the basics of IoT and its architecture. The current IOT issues and issues are discussed in Part 3. Part 4 outlines solutions to key challenges using the latest technology.

II. IOT: OVERVIEW AND ARCHITECTURE

The Internet of Things (IoT) can be defined as a global network of physically connected devices or machines that can interact with each other. As the definition says, IoT is nothing but connected objects that work together to provide intelligent services without human intervention.

The reach of the Internet is extended by IoT. Nowadays, the scope of the Internet includes the connection between computers and computing devices, while IoT extends it to connect different things or physical objects or whatever. These physical objects can be anything we see around us like lights, fans, air conditioners, etc.

These physical objects are equipped with embedded systems, embedded electronics and information technology, so they have a basic computing platform, attached to them and then they act as different nodes of

Specific Internet - IoT in which these nodes communicate with each other and share information to perform a particular task. In this way internet of things works. Based on the connection and sharing of information between different nodes, the layered model of IoT is shown below:

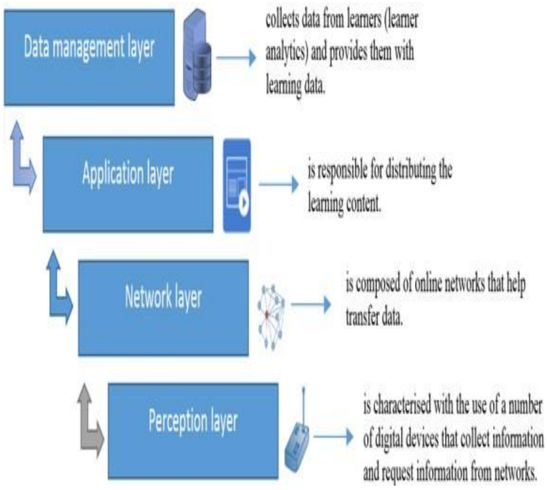
Data management layer
collects data from learners (learner analytics) and provides them with learning data.
Application layer
is responsible for distributing the learning content.
Network layer
is composed of online networks that help transfer data.
Perception layer
is characterised with the use of a number of digital devices that collect information and request information from networks.

Fig 1. Layered model of IoT based on Connectivity.

In phrases of connectivity, commonly there are 3 layers (see Fig.1) i.e., provider layer, nearby connectivity layer and international connectivity layer. For the worldwide connectivity, we've Internet. Using gateway, we are able to hook up with the nearby connectivity layer i.e., distinctive provider vendors and for providerlayer the use of distinctive communique technologies, we are able to hook up with distinctive software regions like agriculture, transportation, fitness care, business, factories, etc.

Beyond the connectivity, there are different gadget that is required to construct IoT this is sensors and actuators. “A sensor may be described as an aspect which senses the modifications withinside the ambient situations or withinside the country of any other item or gadget and sends or methods those facts in precise manner” while “an actuator may be described as an electrical, hydraulic, or pneumatic device (which include relay) which manages the waft of cloth or power”.

The basic IoT workflow is shown in Figure 2. Objects are connected to other objects that interact to provide the same type of service. Physical objects are recognized or detected by the sensor. The sensors detect various parameters like temperature, light, pressure, etc. depending on the sensor used.

The detected information will be sent on a connected system or you can say over the network the information will be transmitted this can also involve the cloud and ultimately the information is transmitted based on what was detected depending on the request that some physical action is performed by an actuator.

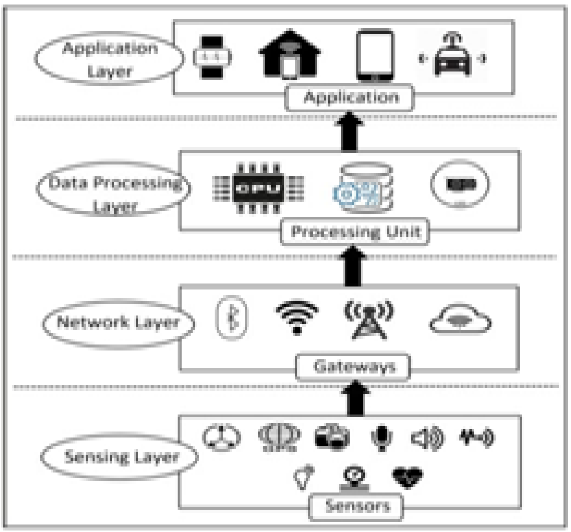

Fig 2. Basic IoT System.

Figure 3 shows the three-layer architecture of IoT, explaining IoT methodologies “The International Telecommunication Union proposes a five-layer IoT architecture, as shown in Figure 3(b) Jia et al and Domingo propose to divide IoT system architecture into three main layers: perception layer, network layer, and service layer.

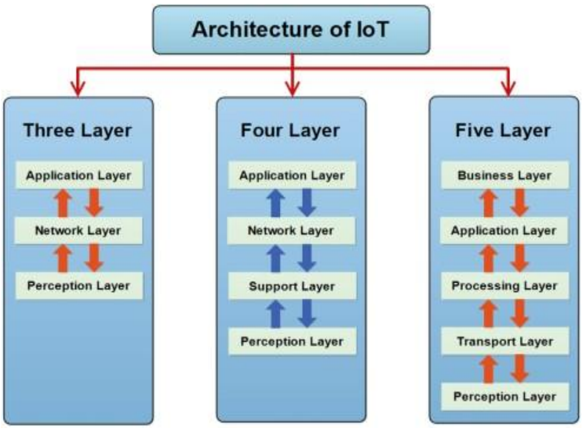

Fig 3. Layered Architecture of IoT.
(a) Three Layer Architecture (b) Four Layer Architecture (c) Five Layer Architecture

Here, the cognitive class of physical objects data collection. In Three-layer architecture, the network layer is required to provide connection between awareness and application layers. It safely transmits data from awareness class to the application layer. But in the Gateway Access Architecture class, used to provide connection between cognitive class and network layer. It organizes objects of communication and systems as well as in the IoT environment. There is another change in the five- layer architecture, the middleware layer providing a more flexible interface between the hardware and the application.

The upper application layer provides services or applications that analyze information received from other layers.

Factors such as network and communication, data processing, security and privacy, scalability, business model, device intelligence need to be considered at the time of architecture design of IOT Figure. The IoT blueprint should be like it provides flexibility, interoperability, respectability, security, portability, measurable quality. Service Oriented Architecture (SOA) is considered a good way to tackle all the good things that have been noted before.

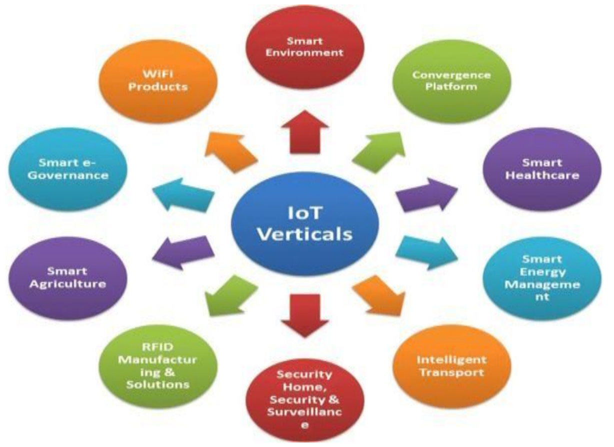

Fig 4. Components of IOT.

1. Sensing Layer:
As we have noticed that IoT is an interconnected system in which physical objects or elements can be linked and controlled remotely. In this layer, wired or remote frames with sensors and RFID tags can detect and share data between different gadgets. Consider the application, special tags or sensors used to detect items and share data.

2. Networking Layer:
The second layer, the network layer, is also known as the transport layer [4]. The main job of this class is to tie everything together. This class is responsible for sharing data between different utilities as it provides availability. It is used to exchange data between the sensor and the data preparation framework. The transmission method can be anything wired or remote, and the innovation can be anything - 3G/4G/5G, WIFI, Bluetooth, ZigBee, etc. depends on the sensor used.

3. Service Layer:
The service layer is responsible for coordinating services and applications in IoT. It contains middleware innovations. For application prerequisites, the middleware innovation is structured. It includes service integration, service discovery, service API, and service management. This layer goes on to form all service-related issues including data sharing, data management, web matching and indexing.

4. Interface Layer:
It is the layer through which users can interact with IoT. Since IoT is the connection between things, it provides different types of communication like machine to machine, machine to person, person to application, etc. So, this layer plays a very important role in IoT SOA. As we all know that a very large number of devices are connected to IoT and all devices may be manufactured by another company, so they do not follow the same protocol or standard.

In this case, problems may arise when communicating with different devices and when exchanging information. Due to this type of problem, IoT applications will not be affected. These types of problems are handled by this class. Finally, a process analysis is performed to evaluate the process.

III. IOT: ISSUES AND CHALLENGES

1. Standardization:
The International Organization for Standardization (ISO) has concluded from the studies it has carried out over the past ten years that standards are essential for the organizational and economic improvement of all companies using them using emerging technologies. It emphasizes quality, safety and respect for environmental policies. It makes users aware of the potential dangers posed by the inconsistent use of production and management techniques. It also provides guidance and insight into specifications, service and maintenance details that can be useful in the absence of technical support, increasing end-user trust.

The standards are one of the key challenges in IoT assessment. IoT objects like sensors, actuators, RFID, etc., built with reasonable scale and low quality, are vulnerable to many security attacks because insufficient data flow increases the vulnerability. like data theft. In addition, due to the lack of standardization of IoT devices, other issues such as privacy, impact of network resources, and interoperability are increasing. Therefore, standardizing IoT devices, objects, and architectures is an essential part of the success of IoT systems.

2. Security and privacy:
Security and privacy are main elements of IoT. It is necessary to secure various IoT network operations such as transport, data processing, storage, and personal operations. Three main security goals: Authentication, Privacy, and Integrity should be targeted to ensure overall security and privacy. IoT security must be applied to all layers of the IoT architecture: the application layer, middleware layer, network layer, and perception layer.

For this reason, the evolution of IoT security architecture and the development of different security and privacy mechanisms are always needed to address security and privacy matters. Various security mechanisms such as authentication, authorization, access control, integrity and security of data need to be improved to focus on overall security. Authentication is one of the important parts of the IoT ecosystem as it must be implemented at every layer of the IoT architecture to ensure overall security.

Appropriate and effective authentication methods should be implemented as required by the different layers to prevent unauthorized access to the object by attackers at the cognitive layer, and from unauthorized access to stored data storage and application at the middleware level and inject malicious code into the system at the application layer.

To securely transfer information between multiple devices, authentication allows the IoT device to secure the identity of the communicating device. With the use of authentication, it is possible to ensure that only trusted users have access to IoT devices and networks at the time of request. It is also necessary to authenticate the data of the communication devices. Although the data is encrypted but not authenticated, anyone can generate fake data and transmit it to the sensor. Therefore, it is necessary to authenticate data communicated between IoT devices to provide security against the generation of tampered data.

Therefore, the lack of proper and effective authentication mechanism implementation at each layer of the IoT ecosystem can lead to a number of potential attacks such as unauthorized access to RFID tags, brute force attacks, attacks, etc. side- channel attack, collision attack, sensor-level data modification, Man struck in the middle attack, etc.

Privacy is also enforced for secure communication of messages between devices on the network. In IoT, users can be people, sensors, objects, etc. The IoT network contains several elements, so it is necessary to ensure that the data from which it is made is only available to legitimate entities. To ensure confidentiality, an access control mechanism or encryption technique must be implemented [11, 13].

Confidentiality and integrity of data must ensure that the data is not modified in any way during transmission. Putting data in while transmitting messages over the network modifies the entire data. Even data stored on an RFID tag or sensor must be protected from modification by an attacker.

RFID tags and sensors only allow a small password for access control to prevent data modification by unauthorized entities, but small passwords can be easily cracked by hackers. Therefore, strong passwords are required for access control to prevent data modification, but handling strong passwords at sensors and RFID tags is another matter.

3. Interoperability:
When several of devices developed by different vendors and using different standards are connected with each other creates the heterogeneous environment which leads to issues of interoperability. IoT supports the use of different devices, resulting in the use of different architectures, networks, and communication protocols, and the generation of data in different formats.

Current Internet scenarios do not support connectivity between heterogeneous devices, which poses the problem of integrating different subsystems, regardless of their native communication protocols.

4. Scalability:
It combines trillions of devices/objects and infrastructure in the same IoT ecosystem, where each object and system use its own architecture, protocol stack, data formats, power processing power, etc., which also poses interoperability problems in a large-scale heterogeneous system. Cloud-based architecture or edge computing can be used as a platform to realize the cloud as a scenario to solve the scalability problem, but edge computing does not support accessibility for a large number of users, which is available with the cloud.

Seamless connectivity is another challenge to deal with scalability while adding devices in an existing network, so it is advisable to implement a network architecture that provides distributed scalability, seamless connection and security.

5. Energy/Power Consumption:
In today's era, the usage of IoT devices increases daily and NIC's (National Intelligence Council of U.S.) foreseen says that in nearer future devices connected with internet will be in billions and therefore energy consumption. The energy required to charge IoT devices, by IoT access points, gateways and sensors as well as the power consumption to process data from various sensors in the IoT infrastructure will be one of the major energy consuming sectors in the future days.

6. Identity Management of connected object:
Each object connected to the IoT network must be uniquely identified among all devices. To do this, a unique identifier such as an IP address or a URL must be assigned to all devices. Once the subject has a unique ID and connects to the network, the subject can be easily tracked, controlled and managed, but the researchers' predictions indicate that the number of subjects connected to the Internet will be more than the number of users.

Internet in the near future. Due to the scalability and portability issues of the object, the static identity system will not work, so the system dynamically assigns a unique number to the object and identity management must be implemented to solve current identification problems.

IV. IOT: FUTURE TRENDS

1. Blockchain Technology:

Blockchain is currently attracting the attention of software scientists since its inception. Blockchain technology [1] is defined as a distributed ledger for storing information across multiple nodes.

Blockchain technology provides a more secure environment for data privacy and security. It uses hashing to encrypt data and digital signatures to authenticate users. By combining a hash function and a digital signature, it authenticates every ledger record. The ledger is distributed in such a way that it can be accessed through any node in the chain. Thus, blockchain technology gets rid of the IoT unified server concept and provides a distributed environment.

The great scale IoT system wishes to perform the analysis, processing capabilities of existing internet infrastructure may not support effectively. These all functions produce distributed habitat & permitting the IoT systems to trace the large range of connected devices.

2. Cloud Computing:

When the network contains several nodes, it is difficult to protect a large amount of data, since it comes from a large number of nodes. Cloud computing provides an efficient solution for IoT by providing storage, processing and other services on large amounts of data and also provides a distributed habitat. The main advantage of IoT with the cloud is that it provides real objects with a distributed habitat.

The cloud provides a transition layer between real things and real-time applications that in many cases hides all the quality and functionality needed to implement the latter. For low-cost data processing and IoT application maintenance, deployment is facilitated by the cloud. Cloud is the most efficient solution for data generated by IoT.

3. Big Data:

In IoT, network communication occurs through sensors, actuators, machines, and other nodes. In IoT, when the network contains more than 1000 nodes, it generates a large amount of data, and managing this data is extremely important. Because data comes from many nodes and each node can have a different environment. Currently, it is very difficult to maintain data quality.

Here, the data can be smart grid, persistence and pollution data after performing analysis, sensor data for traffic management and control, health record monitoring and processing to provide appropriate medical services. In addition, a large amount of data is generated by social networks and global measurements and observations are generated by users. Integrating data from disparate physical, network, and social resources with IoT enables the development of applications and services that can embed situational and contextual awareness into decision-making mechanisms.

4. Distributed Computing:

Distributed computing can be defined as a collection of computers connected in a network to achieve shared computing goals. Distributed computing and parallel computing have many common problems. In the current era, the technology that powers hardware virtualization, distributed computing, and service-oriented architecture is cloud computing. The Internet can be extended into the real world to include everyday things through the use of IoT and distributed computing. Today, most physical objects are mostly interconnected, but can be monitored remotely and also connected to the internet.

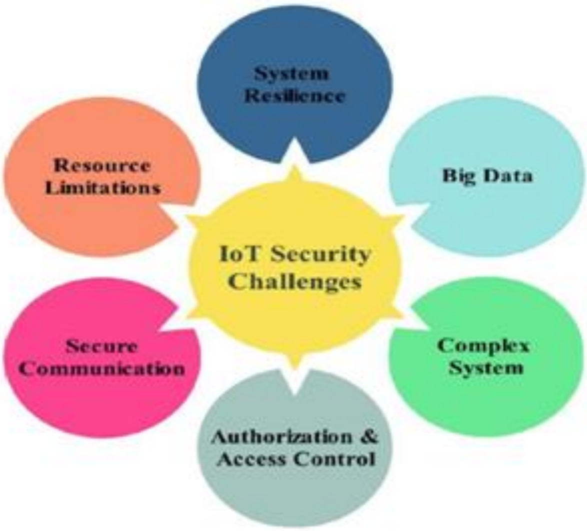

Fig 5. IOT Security Challenges.

V. ACKNOWLEDGEMENT

We would like to express our deep sense of gratitude to the professors Dr. P. Dasharatham, Dr. L. Pratap Reddy, ECE department, JNTUH who are very cooperative and their guidance was invaluable & inspiring in doing this research paper.

VI. CONCLUSION

IoT connects all kinds of objects used in daily life and allows them to interact with each other to make life easier and smarter. In the current scenario, IoT, one of the advanced technologies, provides services like automation, smart city, smart classroom, healthcare, etc.

Although it offers various advantages in different fields, many still face challenges in terms of connectivity, scalability, data security and privacy, etc. Different industries produce various types of sensors, machines, cameras, etc. using different technologies as well as different communication protocols. Devices made with low rates and standards create problems regarding security, interoperability, etc.

Moreover, the increasing rate of connected devices increases the amount of power consumed, which seriously affects the environment. These problems open the door for different researchers to go further in solving challenges to make life easier and smarter. Here, we have identified various IoT issues and challenges that need to be targeted. This document also provides an overview of the latest technologies that can be combined with IoT to solve a number of problems.

REFERENCES

[1] Marianne A. Azer Ahmed Abbokr, "IoT ethics challenges and legal issues," in 12th International Conference on Computer Engineering and Systems (ICCES), 2017.

[2] Sarah A. Al-Qaseemi, Hajer A. Almulhim, Maria F. Almulhim, and Saqib Rasool Chaudhry, "IoT Architecture Challenges and Issues: Lack of Standardization," in 2016 Future Technologies Conference (FTC), SanFrancisco, CA, USA, 6-7 Dec. 2016.

[3] Madhusudan, Abhiraj Singh, and Shiho Kim Singh, "Blockchain: A game changer for securing IoT data," in 4th World Forum on Internet of Things (WF-IoT), 2018.

[4] Pradeep Kumar Mallickb Nallapaneni Manoj Kumara, "Blockchain technology for security issues and challenges in IoT," in International Conference on Computational Intelligence and Data Science (ICCIDS 2018).

[5] Elmustafa Sayed Ali Ahmed Zeinab Kamal Aldein Mohammed, "Internet of Things Applications, Challenges and Related Future Technologies," World Scientific News, 2(67), 126-148.

[6] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," in International Journal of Computer Applications (0975 8887) Volume 111 – No. 7, February 2015

[7] Chin-Feng Lai, Athanasios V. Vasilakos Chun- Wei Tsai, "Future Internet of Things: open issues and challenges," Wireless Networks, Volume 20 Issue 8, 2201-2217 , 13th May 2014.

[8] "Li Da Xu, Senior Member, IEEE, Wu He, and Shancang Li, "Internet of Things in Industries: A Survey"," in IEEE Transactions on Industrial Informatics, vol. 10, No. 4, November 2014.

[9] Mahmoud A. M. Albreem et al., "Green internet of things (IoT): An overview," in IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA), Putrajaya, Malaysia, 2017.

[10] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza and R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)," 2017 Eleventh International Conference on Sensing Technology (ICST), Sydney, NSW, 2017, pp. 1- 5.

[11] Qusay Idrees Sarhan, "Internet of things: a survey of challenges and issues," International Journal of Internet of Things and Cyber- Assurance, vol. 1, no. 1, March 2018.

[12] Kyoochun Lee In Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Buisness horizons, vol. 58, no. 4, pp. 431-440, July-August 2015

[13] 2015.

[14] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 2015.

[15] Sajjad Hussain Shah and Ilyas Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," in IEEE Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2016.

[16] Er. Pooja Yadav, Er. Ankur Mittal, and Dr. Hemant Yadav, "IoT: Challenges and Issues in Indian Perspective," in 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT- SIU), Bhimtal, India, 2018.

[17] Yen-Kuang Chen, "Challenges and opportunities of internet of things," in 17th Asia and South Pacific Design Automation Conference, Sydney, NSW, Australia, 2012.

[18] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in 10th International Conference on Frontiers of Information Technology, Islamabad, India, 2012.

[19] Chunsheng Zhu, Victor C. M. Leung, Lei Shu, and Edith C.-H. Ngai, "Green Internet of Things for Smart World," IEEE Access (Volume: 3), 2015