IOT Challenges, Solution Framework, And Implementation

Pooja Mittal [1,*], Dr. Monika Sharma[2] and Mr. Amrit Nath Thulal[3]

[1] Master in Computer Applications, AIIT, Amity University Noida Uttar Pradesh, India
[2] Associate Professor, AIIT, Amity University Noida Uttar Pradesh, India
[3] Assistant Professor, AIIT, Amity University Noida Uttar Pradesh, India

Abstract

The Internet of Things is a vast growing technology that is almost applicable in all fields and has simplified our lives. IOT is being used everywhere these days, including in smart cities, smart environments, security, smart business processes, smart agriculture, healthcare, and many more fields. Being able to cover various fields, is very challenging and presents various problems. This paper highlights IOT components, building blocks, enabling technologies, characteristics, applications, and products, as well as the issues encountered by them and lastly their causes. It brings forward seven steps of proposed solutions for handling and eliminating the problems encountered by almost all IOT devices and applications. The main aim of this paper is to provide the solution for all the issues which have been talked about for years but could not be able to resolve.

Keywords: Internet of Things (IoT), Issues, Enabling Technologies, Security, Privacy, Applications, Implementation, Proposed Solution

Received on 30 May 2023, accepted on 23 August 2023, published on 28 August 2023

doi: 10.4108/eetiot.v9i3.3408

*Corresponding author. Email: poojamittal2842@gmail.com

1. Introduction

It's been a long while since the expression "IoT" was first discovered. Our lives are quickly driven into a fictional universe characterized as a virtual space given the quick improvement of the Web and correspondence advancements. It is capable and versatile enough to change with the surroundings with ease[1]. In the virtual world that the network provides, individuals can work, shop, and manage pets and plants. Human activities, however, cannot be fully executed through the services provided in the fictional space because people exist in the real world and services provided in the virtual world cannot entirely fulfill human needs. The difficulty of growing into an imaginary space limits the Internet from upgrading its services. IoT connects the real world to the virtual world which helps in overcoming limitations.

Sensor network technology places new requirements on Internet technology because it is based on a large number of affordable sensors and wireless communication. In this context, it is improving due to the development of cutting-edge wireless technology. The presence of various objects, including RFID, NFC, sensors, actuators, and mobile phones are the basic principle behind this approach. The purpose of this article is to present existing Internet of Things (IoT) applications, technologies, and Issues [2] and to eliminate these issues we have proposed seven steps of the solution. IoT is a network that can store and exchange data online without the assistance of any human beings. It requires hardware, software, connectivity to the internet, electronic components, and electricity.

2. Literature survey

S. Choudhari, T. Rasal, S. Suryawanshi, M. Mane, and S. Yedge, "Survey Paper on Internet of Things: IoT,". This author has provided an overview of the Internet of Things. The first author introduced the topic and talked about the basics of IoT and emerging technologies. Technology included is Radio Frequency Identification (RFID), GPS, Machine-to-Machine Communication (M2M), Vehicle-to-Vehicle Communication (V2V), RFID Reader, and Internet Protocol (IP). Secondly discussed algorithms, elements, protocols, challenges, and applications in IoT. The main focus of this paper is on technologies and their specifications[1].

J. S. Kumar and D. R. Patel, "A Survey on the Internet of Things: Security and Privacy Issues. In this author has provided an overview and background of the Internet of Things. Firstly, author gives the definition and Evolution of IoT with the architecture and protocols. The paper briefly explains all the applications of IoT. In this paper, the focus was briefly on the IoTs applications in medical (health care), smart homes, and intelligent community security systems (smart city). The main focus of this paper is on privacy and security concerns in IoT[2].

M. Kavre, A. Gadekar, and Y. Gadhade, "Internet of Things (IoT): A Survey,". This author has provided an overview of the Internet of Things. A brief discussion is done on technologies like Radio frequency identification, Wireless sensor networks, and cloud computing. In addition, architecture with all its layers has been discussed. The other half of the paper includes services, applications, issues, and challenges. The main focus of this paper is on the four-layered architecture[3].

S. Shukla, N. K. Chaurasia, and S. K. Vishwakarma, "A Literature survey on Internet of Things (IoT), with its Evolution,": In this author has provided an overview of the Internet of Things. Firstly, the author introduced the topic and talked about the basics of IoT, evolution, architecture, and application. The second half of the paper gives a literature survey of the work done by scientists around the globe. The main focus of this paper is on providing a literature review of other authors[4].

Ala. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,". In this paper, the author provides an overview of the Internet of Things by giving emphases on enabling technology, protocols, and applications. They give a brief discussion on the five-layer architecture namely the Objects layer, object abstraction layer, service management, application, and business layer. They also included Iot elements, protocols, applications, and challenges[5].

Prof. Sathish and Dr. S. Smys, "A Survey on Internet of Things (IoT) based Smart Systems,". In this paper, the author focuses on the application of iot in different areas like smart living, smart agriculture, smart parking, smart cities, smart industry, smart environment, and smart energy. they also give detailed descriptions of how and which technology to be used to make smart home architecture, home automation, and smart cities[6].

V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,". This paper mainly focuses on security threats and solutions. firstly they discuss security issues in different application areas. Then they discuss all the security concerns present in different layers of IoT in detail and last they provide four technologies Blockchain, fog computing, edge computing, and machine learning as a solution to enhance security in IoT [7].

P. P. Ray, "A survey on Internet of Things architectures,".In this paper, the author focuses on the architecture of IOT. the architecture is presented in such a way that will solve real-life problems. This paper gives a brief about IoT, challenges, applications, and technologies.[8].

K. Singh and D. D. Singh Tomar, "Architecture, enabling technologies, security, and privacy, and applications of internet of things: A survey,". This paper focuses on how the diversion of fog computing and IoT. This paper gives a detailed review of IoT, its application, privacy, and security issues, challenges, enabling technology, and architecture.IT also cover 3-layer and 4-layer architecture and also it gives detailed enabled technologies in different layers of IoT.futhermore application like smart cities, and home. grid, transportation has been discussed. The main purpose is to provide a deep understanding of IoT and its integration with fog computing[9].

3. Components

1. Sensors/devices: Real-time data are gathered from the surroundings with the help of sensors or devices. Sensors may collect different data in many ways, including via video feeds and basic temperature sensors[3].
2. Connectivity: Once the data is collected, then the gathered data is sent to the cloud infrastructure. To link a sensor/device to a cloud, various networks such as satellite, Bluetooth, Wi-Fi, and WAN are used.
3. Data processing: After data has been gathered and sent to the cloud, the software starts processing collected data. This process helps to check the temperature of the air conditioner or heater or can identify objects in videos by using computer vision.
4. User interface: After the collected data has been processed, now the users can get benefitted from it and have that information on their phones we can do this by sending notifications to the users in the form of emails, text messages, or alarm triggers.

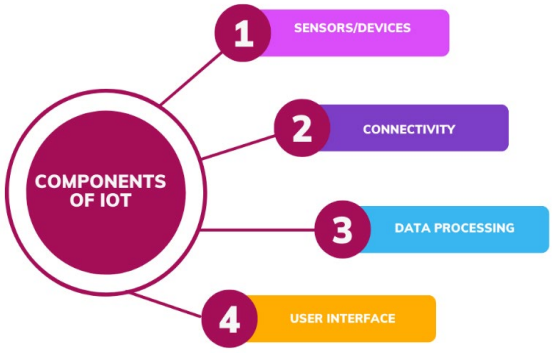


Figure 1: Components of IoT

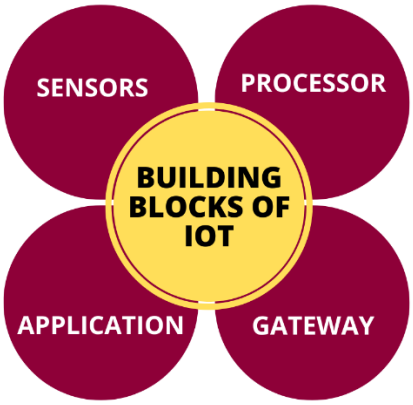


Figure 2: Building blocks of IoT

4. Building blocks

The four components of an IoT system are sensors, processors, gateways, and applications.

1. Sensors: Sensors are the backbone of the IoT. Its primary motive is to gather data from the surroundings and send it to the database or storage. Real-time data is gathered and sent to processors. Many different types of sensors, such as gas, water quality, motion, moisture, image, etc., have various functionalities.
2. Processor: Processors are the functionality of IoT devices. It processes the raw data collected by sensors from the environment into useful information. In a nutshell, we can say that the collected is useless unless the processor comes into the picture and provides intelligence to it[9].
3. Gateway: Gateways provide a route for processed data to be transferred to a database or network storage. The ability to communicate and connect to the internet is crucial for IoT systems. Lan, Wan, and Pan, for example.
4. Application: The application uses the data gathered by the sensors and provides an interface for users to interact with the data. Users have full control over the application. These might also be connected to a cloud platform[4]. Examples include applications for industrial control hubs, security system controllers, and smart homes.

In a narrow sense, sensors gather raw data from their environment and transfer it to a processor. The processor then transforms the raw data into useful information. Then, using device connectivity, the gateway sends the data to a remote cloud application or database system.

5. Technologies

1. RFID (Radio Frequency Identification): RFID is a wireless technology that is used to track and identify objects. Tag and reader are its two components. The object we wish to track is given an RFID tag, and the receiver detects the tag to identify the object. The tag and receiver have a 1-meter range. There are two types of RFID tags: active tags and passive tags. RFID technology functions in a similar way to bar codes and magnetic chips in ATM cards. The RFID devices must be scanned to retrieve the identifying information, just like a bar code or magnetic strip is read to obtain information.
2. NFC (Near Field Communication): It is a form of wireless technology derived from RFID technology. This technology involves an NFC receiver and an NFC tag. The information on an NFC tag is read by an NFC receiver. It has a 10 cm range and a 106,212,424-kbps data rate.
3. Zigbee: It is a cheap and power-efficient wireless technology. It is primarily utilized in systems that are battery enabled. It employs many topologies, including stars, cluster trees, and mesh topography. Data is transmitted at a rate of 250 kbps across a 100-meter distance.
4. LoRaWAN (Long Range Wide Area Network): It is a low-cost, low-power technology with a range of 10 to 15 kilometers, but in comparison to other technologies, its data transmit speed is lower, at 300bps to 37.5 kbps without any license data can be sent on various frequencies, including 169 MHz, 433 MHz, 868 MHz (Europe), 915 MHz (North America), and 865 MHz to 867 MHz in India.
5. 6LoWPAN (IPv6 over Low Power Wireless Personal Area Network): It is a wireless sensor network that is used in industrial monitoring, agricultural, and home automation. It adheres to the IPv6 protocol.

6. GSM (Global System for Mobile Communication):7. It is a digital and open cellular technology. To deliver voice and data it uses the 850MHz,8. 900MHz, 1800MHz, and 1900MHz frequency bands Time Division Multiple Access (TDMA) technologies are used in the development of gsm technology for communication purposes.
7. GPRS (General Packet Radio Services): For wireless and cellular network communication services, GPRS is the finest packet-switching protocol. An essential component of GSM network switching is the GPRS system. We can email, send multimedia messages, and make video calls utilizing GPRS.
8. LTE (Long Term Evolution): It is a 4g wireless standard, which is quicker than 3G technology. 10 to 15 Mbps and 15 to 20 Mbps are its typical downloading speed.

6. Characteristics

IoT depicts those devices which are connected through the internet. IoT includes those devices which can send and receive data through a wireless network.

1. 1. Connectivity: - Connectivity is one of the key aspects of IoT. IoT devices and their components like sensors, compute Engines, Data Hubs, etc are connected. Networks like radio waves, Bluetooth, Wi-Fi, Li-Fi, and others are used to connect IoT devices.
2. Intelligence: IoT is intelligent since it uses several algorithms. IoT mainly uses machine learning and big data analytics to make smarter decisions. Data is used and business decisions are based on them depending on the circumstances. By analyzing this, we can conclude that IoT is clever and smart.
3. Sensing: - Without sensors, it would be impossible for us to communicate, store, or receive data. Only with the aid of sensors are we able to measure or identify environmental changes. Humans can understand and analyze the conditions based on prior experiences, but the Internet of Things (IoT) needs current analog signals, which are provided by sensors, to analyze or function properly. In IoT, we employ electrochemical, gyroscopes, pressure, light, RFID, GPS, and other sensors to gather data and analyze issues[5].
4. Dynamic nature: The nature of IoT is dynamic. In the IoT, data is gathered and transformed so that it may be applied to business choices. The nature of an IoT component should be dynamic to gather and process data, i.e., it should change.
5. Scale: Depending on the requirements, it shifts from a small to a large scale. IoT operates on a small scale in homes, whereas it operates on a large scale in factories or businesses[5].
6. Security: Security is one of the key characteristics of IoT. Security risks are present in IoT devices, and these risks must be avoided. Sensitive information is typically transferred with a significant risk of the hacker or attacker manipulating or stealing the data. IoT systems are created in a way that uses a firewall or VPN to stop these risks.

Communication: IoT devices are connected to the internet and can communicate with one another.
Scalability: As there is an increase in the use of IoT devices, the IoT setup should be developed in such a manner that it can handle expansion.

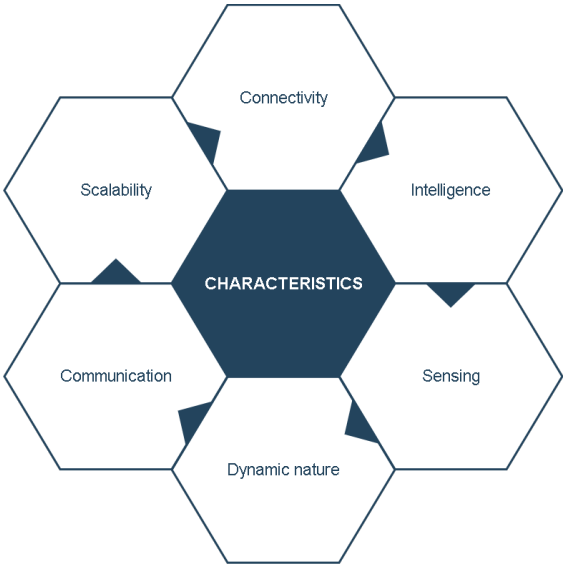


Figure 3: Characteristics of IOT

7. Application

Daily applications for IoT include those in lifestyle, retail, city, building, transit, agriculture, healthcare, environment, and energy. Smart homes, smart cities, wearable technology, smart hospitals, and others are some of the uses[6].

1. Wearable: One of the most popular types of IoT is wearable technology, such as smartwatches, glucose monitors, GPS tracking belts, and heart rate monitors. These gadgets have sensors that gather data, and because of their compact size, they use less energy.
2. Health: In health care, it is helpful for both patients and doctors. In hospitals to track patients' blood pressure, temperature, and other vital signs smart beds are used which have sensors in them.
3. Monitoring traffic: IoT can also be used to keep an eye on traffic. We can track vehicle speed, evaluate traffic, and if someone is not obeying traffic laws, a computer can identify them and instantly issue a challan.
4. Agriculture: IoT is applied in agriculture to properly evaluate soil quality. To monitor and gather data, sensors are deployed on farms. Data about the soil's moisture content, acidity, nutrients, and humidity can be gathered. After examining this data, problems that will arise shortly can be avoided and crop quality can be improved. Animal tracking aids in keeping an eye on creatures in wide spaces.
5. Smart home: All of the home's elements, including the air conditioner, television, refrigerator, led bulbs, fans, doors, washing machines, etc., have been converted into

smart appliances using the Internet of Things, making life much more convenient and comfortable.

6. Smart city: IoT is employed in various cities for traffic management, trash management, water distribution, electricity management, and pollution monitoring technologies[7].
7. Industrial Automation: Automation refers to the completion of a work without the assistance of a human. Making a product that is effective and efficient is crucial in every company, and IoT facilitates this[8].

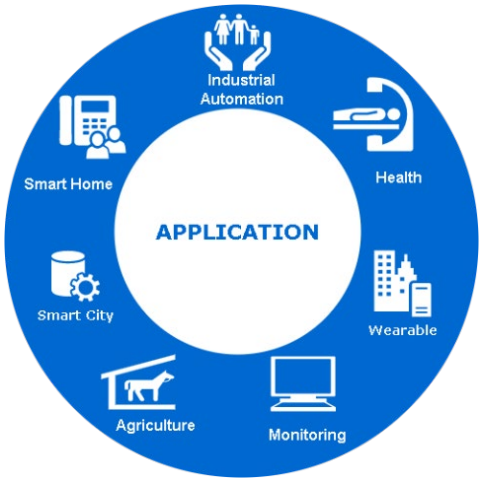


Figure 4: Applications of IoT

8. IoT-devices

1. Smart Home Devices: smart home devices such as smart thermostats, lighting systems, door locks, and security cameras offer remote control and automation features.
2. Wearables: IoT wearable devices like fitness bands and smartwatches can track activity, heart rate, sleep habits, and much more.
3. Connected Cars: To offer connectivity, entertainment, security, and safety features, as well as to connect multiple systems and exchange data, cars are also connected to the Internet of Things (IoT).
4. Industrial IoT: According to reports, IoT-based industrial automation increases production efficiency by up to 72% and decreases accidents by up to 50%.
5. Healthcare IoT: Iot usage in healthcare is increasing rapidly in the form of remote monitoring devices and health wearables. It helps in tracking medication, monitoring patient health, and providing automated emergency response[8].
6. Smart Farming: Products like crop monitoring systems, soil and moisture sensors, and farm management software are used in the agriculture sector to assess soil type, among other things.
7. Energy Management: These days, smart grids and IoT-enabled energy management systems regulate and track energy usage in buildings, greatly reducing energy costs.

9. Issues encountered from applications and products

With their innovations, IoT has significantly improved our quality of life. However, while building and deploying IoT-based devices there are still several challenges to be overcome. Several of these problems include:

1. Security: The biggest concern in iot devices is security as every one of the devices is associated with the internet, they are powerless against hacking and cyberattacks as a result of which unapproved access and command over the devices should be possible which likewise prompts loss of sensitive information.
2. Privacy: The primary problem with IoT devices is privacy. IoT devices gather a lot of personal information, including location, preferences, and others, which can be sold to a third party or used as leverage in extortion[9].
3. Interoperability: It may be challenging to create interoperable devices due to the lack of standardization for data exchange in IoT technology. This could provide a challenge when developing complex IoT systems that need the cooperation of multiple devices.
4. Complexity: All Internet of Things (IoT) devices are built on a little specialized knowledge, making them complex. It could be challenging for the end user to operate these gadgets alone, which creates a barrier[10].
5. Compatibility: As technology changes, older devices are incompatible with newer ones, creating compatibility issues that get in the way.
6. Power consumption: Most IoT gadgets require excessive amounts of electricity and are dependent on batteries or other power sources, which restricts their usefulness.
7. Data analytics: IoT devices capture a lot of data, which makes managing and processing it quite difficult. Real-time data analysis thus becomes difficult.

10. Seed for the issues

1. Security Vulnerabilities: IoT devices collect a large quantity of data every day, and if it is not adequately protected, it could be hacked or manipulated, which could result in data breaches, identity theft, and a loss of customer trust.
2. Interoperability: Products from the IT industry are built on several technologies and protocols, which can lead to connection problems, compatibility problems, and data silos.
3. Data Overload: IoT generates a tremendous amount of data, some of which may not be accurate or relevant if not properly processed. This can also lead to slow response times, lost data and even system crashes.
4. Power Limitations: IoT devices frequently run on batteries or are dependent on minimal power sources. Their functionality and performance may be hampered by this restriction.

5. Complexity: Because of their complexity, designing and managing IoT solutions can be difficult. It takes a lot of development labor and money to ensure that the parts, sensors, and communication protocols operate together seamlessly.
6. Privacy challenges: IoT devices have the potential to gather private information that, if improperly managed, could result in privacy violations and the violation of individual rights.
7. Lack of standardization: Lack of standards in the IoT sector can cause interoperability problems, vendor lock-in, and a lack of transparency[11].
8. Regulatory Compliance: IoT goods must adhere to a variety of regulations, which can change from one region to another. Meeting these needs may increase the complexity of development, design, and testing.

All in all, it tends to be challenging to ensure that IoT-based merchandise is secure, viable, versatile, dependable, private, and financially effective, and blunders here can immensely affect both producers and customers. To ensure that IoT-based goods continue to be viable and trustworthy solutions as IoT technology develops, it is critical to address these concerns proactively[12].

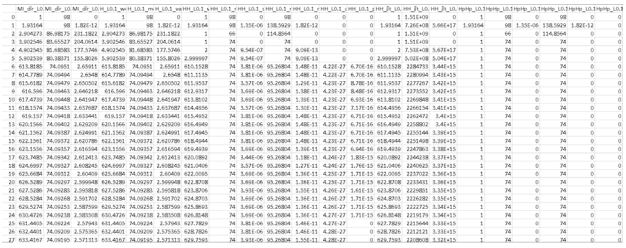
11. Proposed solutions

1. Identify the issue: the first and most important steps that should be taken are to identify the issue and why the product is not working properly. The problem that occurs in iot products can be because of many reasons such as connectivity issues, data security concerns, compatibility issues, or software bugs. The problems can be solved in many ways like taking feedback from the customers, or through testing and troubleshooting.
2. Analyze the issue: once it is clarified what the issue is, the next step is to examine the problem in detail. The problem can be investigated by collecting and analyzing the data. Now we have to understand the mainspring of the issue as well as how the users and products are getting affected by it. This will be the main move toward taking care of the issue.
3. Develop a plan: after analyzing the issue now a plan needs to be prepared to address the issue. It may involve developing new software, replacing faulty hardware, or making changes to the design of the product.
4. Implementation of the plan: after identifying and analyzing the issue and developing a plan now it's time to implement the plan i.e., start making necessary changes to the product. It includes updating the firmware, replacing components, or making software configuration changes.
    a. Update software: if the issue is related to a software bug, then the solution can be updating the software which will typically solve any security or compatibility issues.
    b. Improve connectivity: If there is a connectivity issue then a durable network infrastructure may be the solution. A more reliable network can help improve connectivity and eliminate related issues.
    c. Boost security: It's critical to identify and repair the affected point if a security breach is posing issues. Additional security precautions including strong passwords, encrypted messages, and VPN technology can help stop the recurrence of similar problems.
5. Test and Validate: once all the necessary changes are made, now to ensure all the problems are fixed, the product needs to be tested and validated. This includes both computerized and manual testing, as well as get-together input from clients.
6. Monitoring and Maintaining: finally, it is important to monitor the product and maintain the product to ensure it works properly and the issue is fixed permanently. This involves testing, debugging, and updating new issues that may arise.
7. Develop a contingency plan: after resolving all the issues and making a bug-free product, a plan must be developed which addresses future steps that need to be taken care of once the product has been used by customers which may include updating the software as per new technology so that product can cope up with the environment.

Figure 5: Proposed Solution Framework

12. Implementation

Let's take a scenario of customer satisfaction detection. So what we have done is, we have taken the dataset of a company's product. The data is collected by the sensors of the product from the environment. It includes feedback from the customers, tracking their usage, tracking where people are having problems in using the product, etc based on which implementation has been taken forward. with the help of a decision tree classification algorithm in supervised learning, we have tried to find the accuracy of the product. The purpose of using this algorithm is to get a decision that is easy to understand and has human thinking ability.



First, we train the model and after training the model, using the decision tree classification algorithm we found out the accuracy of the product. If the accuracy of the product comes near to 0 then that indicates that we can move forward with the product and move forward on 3 steps which is developing a plan. If not then we still have to work on the product and find out what is preventing it from performing appropriately.

13. Result and analysis

```
[ ] from sklearn.model_selection import train_test_split
    x_train, x_test, y_train, y_test = train_test_split(X, Y, test_size=0.33, random_state=42)

[ ] from xgboost import XGBClassifier
    from sklearn.metrics import accuracy_score
    from sklearn.tree import DecisionTreeClassifier

    xgb_model = DecisionTreeClassifier().fit(x_train,y_train)

    training_score = accuracy_score(xgb_model.predict(x_train),y_train)
    testing_score  = accuracy_score(xgb_model.predict(x_test),y_test)

    print(training_score)
    print(training_score)

    1.0
    1.0
```

The Proposed Solution provides seven steps which include identifying the issues to develop a plan which will help tackle the issue which arises after the product has been used by the customer.
In the dataset, the customers have given feedback on the product what problems they have faced, etc.
In the example, the accuracy of the product is 1.0 which state that we can move future with the product i.e. first two steps of the proposed solution has been covered which is identifying and analyzing the issue. Now we can move to the next step which is developing a plan for product correction. But if the accuracy was less then it would

determine that the product needs more work to be done on it. So the issue is not resolved and still need to analyze the dataset and other parameters to find out the issues. With this proposed solution we are analyzing iot products and applications using AI to improve further challenges.

14. Conclusion and future scope

IoT is being used everywhere these days, including in smart cities, smart environments, security, smart business processes, smart agriculture, healthcare, and many more fields. Everything required to make it a reality has been covered in this paper [1]. Nowadays internet applications have become a part of our life, still there are extensive obstacles and restrictions on their use which need to be identified. This paper introduces a seven-step proposed solution to eliminate the issues which stop IoT products from functioning properly and also to solve all the issues which come in the way when the product reaches and is used by customers. It analyzes using Artificial intelligence to improve future challenges. After all the work is done, there is space for improvement. This paper only covers the implementation of the first two steps, implementation of the future 5 steps still needs to be done. IoT is playing a great role in today's world but for a better future, all the issues needed to be identified and enhanced, and the proposed 7 steps solution will help in doing it.

Bibliography

[1] S. Choudhari, T. Rasal, S. Suryawanshi, M. Mane, and S. Yedge, "Survey Paper on Internet of Things: IoT," *Int. J. Eng. Sci. Comput.*, vol. 7, no. 4, pp. 4–7, 2017, [Online]. Available: http://ijesc.org/.

[2] J. S. Kumar and D. R. Patel, "A Survey on the Internet of Things: Security and Privacy Issues," *Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, 2014.

[3] M. Kavre, A. Gadekar, and Y. Gadhade, "Internet of Things (IoT): A Survey," *2019 IEEE Pune Sect. Int. Conf. PuneCon 2019*, no. October 2021, 2019, doi: 10.1109/PuneCon46936.2019.9105831.

[4] S. Shukla, N. K. Chaurasia, and S. K. Vishwakarma, "A Literature survey on Internet of Things (IOT), with its Evolution," vol. 2, pp. 414–421.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[6] Prof. Sathish and Dr. S. Smys, "A Survey on Internet of Things (IoT) based Smart Systems," *J. ISMAC*, vol. 2, no. 4, pp. 181–189, 2020, doi: 10.36548/jismac.2020.4.001.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," vol. x, 2019.

[8] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, 2018, doi: 10.1016/j.jksuci.2016.10.003.

[9] K. Singh and D. D. Singh Tomar, "Architecture, enabling technologies, security and privacy, and applications of internet of things: A survey," *Proc. Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), I-SMAC 2018*, pp. 642–646, 2019, doi: 10.1109/I-SMAC.2018.8653708.

[10] A. Yacob, "A Review of Internet of Things (IoT): Implementations and Challenges," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1.3, pp. 373–376, 2020, doi: 10.30534/ijatcse/2020/5891.32020.

[11] Avanti Pawar and Ajay Lahane, "Design and Implementation of IoT based Smart Surveillance," *Int. J. Eng. Res.*, vol. V9, no. 04, pp. 562–567, 2020, doi: 10.17577/ijertv9is040501.

[12] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Comput. Networks*, vol. 144, pp. 17–39, 2018, doi: 10.1016/j.comnet.2018.07.017.