Internet of Things (IoT): Importance, Features, Working Procedures, Applications, Security, Risks and Challenges

[1]Rafat Ara, [2]Md. Abdur Rahim

[1,2]Assistant Professor, Department of Computer Science and Engineering, German University Bangladesh, Gazipur, Bangladesh

ABSTRACT

In this paper, we want to introduce the notion of the Internet of Things (IoT) broadly and review the primary obstacles of the IoT environment by emphasizing the recent research orientations in this field. IoT, or the Internet of Things, is a new technology that has recently surfaced. It expresses a modern wireless telecommunication network and is defined as an intelligent and interoperable node connected to a dynamic global infrastructure network. It also aims to realize the connectivity concept of anything at anytime, anywhere. Here, in this paper, we clarify the fundamental ideas behind the Internet of Things. We also look at the powerful other current or emerging IoT technologies. We are addressing numerous likely future difficulties while providing a comprehensive multifaceted study on IoT adoption. Furthermore, this article outlines the primary applications, security, risks and challenges for the Internet of Things.

Keyword: *IoT, Internet of Things, Technologies, Application, Risks, Challenges.*

1. INTRODUCTION

Many people consider the twenty-first century to be the information era, and the Internet's pervasiveness in many facets of our lives has opened up new avenues for technological advancement. The way we live has been altered by technological growth, and digital information is now a societal infrastructure. Technology is all around us; computers may be found in our phones, watches, cars, entertainment systems, and household appliances. The concept of the Internet of Things (IoT) has the potential to fundamentally change how we interact with technology. Science fiction once held the promise of a world where every technological gadget in our environment is a part of a single, global network. However, IoT is not just making waves in the nonfiction space it's sweeping the globe. IoT gadgets are becoming widely available. IoT devices are predicted to have the biggest influence on our daily lives in our (smart) homes, where they have begun to migrate from our workstations.

The majority of smart home equipment will be commonplace appliances like toasters and kettles. Kevin Ashton of Procter & Gamble most likely invented the phrase "Internet of things" in 1999.[1] Firstly, he thinks the term "Internet for things" is more appropriate since it stresses the importance of radio-frequency identification (RFID) in the Internet of things, which would enable computers to control every single thing. According to Cisco Systems, the Internet of Things was "born" between 2008 and 2009, with the definition simply referring to the fact that people interact with it more than with each other [2]. The term "internet of things" has become popular in the fast-paced world of today. The Internet of Things (IoT) makes it possible for different devices to communicate with one another online. This guarantees that the devices are intelligent and that the data is sent to a centralized system, which will monitor and act in accordance with the mission assigned to it. IoT applications include electricity grids, smart buildings, entertainment, healthcare, and transportation [3]. The Internet of Things (IoT) is anticipated to drive future technical advancements and see a massive increase in use in the upcoming years. From a security standpoint, the Internet of Things will confront more difficult obstacles. For example: (1) the Internet of Things (IoT) expands the concept of the "internet" to include the traditional internet, sensor networks, mobile networks, and so forth; (2)

all "things" will be linked to this "internet"; and (3) these "things" will interact with one another. In this paper we will discuss about the basic, Elements, Importance, Working procedure, Applications, Security, Risks, and Challenges of IoT.

2. INTERNET OF THING OR IOT

The Internet of Things, or IoT, is a network of interconnected computers, digital and mechanical devices, items, animals, and people that can transfer data over a network without requiring human-to-human or human-to-computer interaction. All of these devices are assigned unique identifiers, or UIDs. The term "thing" refers to any natural or artificial object that can be given an IP address and be able to transmit data over a network, such as a person with an implanted heart monitor, a farm animal with a biochip transponder, an automobile with sensors to warn the driver when tyre pressure is low, or any other combination of these.

IoT is being used by businesses across a range of industries more and more to boost productivity, enhance decision-making, better understand consumers to provide better customer service, and raise the value of the company. The idea of common physical objects being able to identify themselves to other devices over the internet is known as the internet of things (IoT), which is a computing concept. The phrase is most strongly associated with RFID as a communication technology, while it can also refer to other wireless, sensor, or QR code technologies.

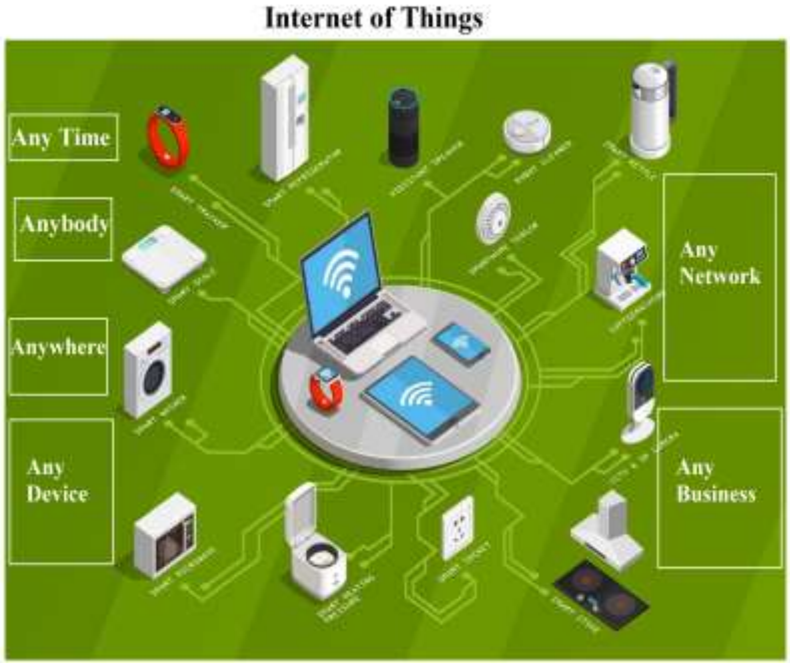

Fig -1: IoT

3. THE IMPORTANCE OF INTERNET OF THINGS

The Internet of Things (IoT) is a widely accepted and appreciated technology that reduces human effort and provides vast amounts of information, allowing people to feel more in control of their surroundings. It has also gained popularity through product prototype development, where entrepreneurs can create affordable, market-ready IoT devices with professional engineering teams, ensuring successful product development.

IoT devices offer four significant benefits in daily life:

1. Better life quality: IoT devices improve communication, allowing people to dedicate more time to other activities and focus on more important tasks. They also offer automation of processes, such as turning on lights,

opening garage doors, and adjusting thermostats. Wearable devices can help users work out without worrying about burned calories.

2. Data-driven decisions: IoT devices enable decision-making based on collected data, such as improving crop quality by measuring soil, humidity, and nutrients. The collected information helps identify potential problems and make informed decisions.

3. Real-time monitoring: IoT devices can monitor the quality of goods at home, allowing homeowners to know when to replace items without constant checking. The IoT-based Asset Tracking and Monitoring market is projected to grow from USD 3.9 billion in 2022 to USD 6.6 billion by 2027, allowing companies to track their assets in real-time and identify internal risks and potential dangers.

4. COMPONENTS OF IOT

In its literal sense, the term "Internet of things" denotes the plurality of its components and their sum—that is, intelligent objects—in this case. However, the following constituents are not included in this list as they form the foundation of the Internet of Things: Digitized Repository, Moving Mechanism Transceivers, Objects, and Sensors.

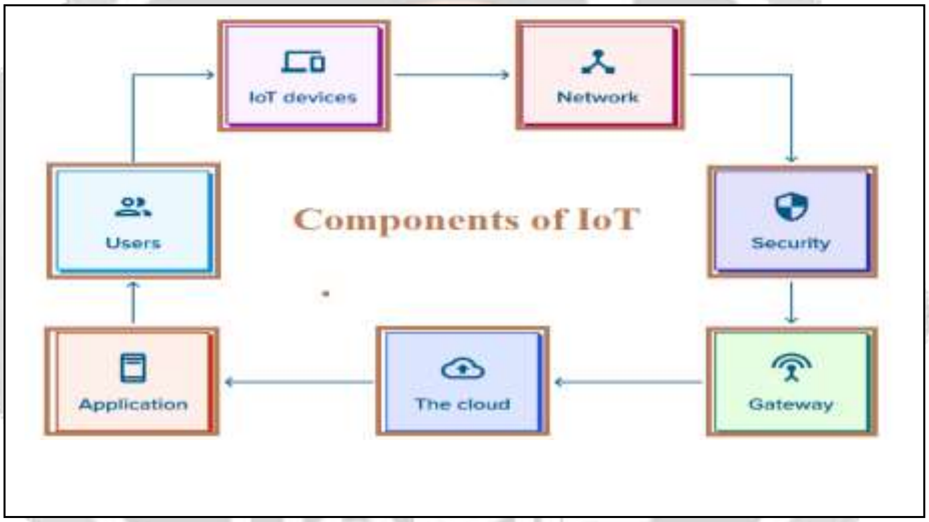

Fig -2: Components of IoT

5. FEATURES OF THE INTERNET OF THINGS (IOT)

Several of the Internet of Things' most well-liked features include:

a. Brainstem
b. Networking
c. Adaptability
d. Vast magnitude
e. Perception
f. Inconsistency
g. Safety

a. Brainstem

IoT is intelligent because it combines hardware, software, and algorithms. The Internet of Things gains enhanced capabilities via ambient intelligence, enabling objects to respond intelligently to specific situations and supporting them in completing specific tasks. Despite the widespread use of smart technologies, intelligence in the Internet of Things is limited to the means of communication between devices; graphical user interfaces and conventional input techniques are the primary ways of facilitating communication between users and objects. The "intelligent spark" that gives a product experience intelligence comes from the combination of algorithms and computing (i.e., software & hardware). Think about the Misfit Shine fitness tracker in comparison to Nest's smart thermostat. Through the Shine experience, computational workloads are split between a smartphone and the cloud. For the AI that makes them intelligent, the Nest thermostat has more processing power.

b. Networking

By connecting commonplace devices, connectivity enhances the potential of the Internet of Things. These objects' connectivity is essential because even basic interactions between them advance the IoT network's collective intelligence. It permits network connectivity and interoperability in the objects. Through the networking of smart objects and apps, this connection may open up new markets for the Internet of Things. It takes more than just sticking on a WiFi module to be connected in the Internet of Things. Connectivity makes networks compatible and accessible. While compatibility offers the shared capacity to create and consume data, accessibility refers to joining a network. This is Metcalfe's Law, and it applies to the Internet of Things, which explains why it sounds familiar.

c. Adaptability

Gathering data from its surroundings is the main function of the Internet of Things, which is made possible by the constant changes that occur in and around the devices. These devices have dynamic states, including as connecting and disconnecting, sleeping and awakening, and changing temperature, position, and speed with relation to other devices. The quantity of devices also varies dynamically with a person, place, and time, in addition to the state of the gadget. The context of devices, which includes location and speed, as well as the states of the devices themselves—such as sleeping and waking up, connected and/or disconnected—change dynamically. Furthermore, the quantity of devices may vary on a dynamic basis.

d. Vast magnitude

Compared to the number of devices connected to the Internet now, there will be a significantly greater number of devices that need to be managed and communicate with one another. It becomes more important to manage the data produced by these devices and understand it for application needs. The anticipated research from Gartner (2015), which projects that 6.4 billion connected items will be in use globally in 2016—a 30% increase from 2015—and that 5.5 million new things will be connected every day underlines the huge magnitude of IoT. Additionally, according to the estimate, there will be 20.8 billion connected devices by 2020. Compared to the devices connected to the current Internet, at least an order of magnitude more gadgets will need to be controlled and speak with one another. Handling the produced data and interpreting it for use in applications will be much more important. Both efficient data management and data semantics are relevant here.

e. Perception

Without sensors, the Internet of Things would not be able to monitor and gather data about changes in its surroundings, report on its conditions, or even interact with it. A true awareness of the physical environment and its inhabitants can be created with the help of sensing technologies. The sensing data is just analogue input from the real world, but it may provide us a deep insight of our intricate environment. We frequently take for granted our senses and our capacity to perceive and comprehend the people and objects around us. Sensing technologies provide us the ability to design experiences that truly represent our awareness of the physical environment and the people who inhabit it. This is merely the physical world's analogue input, yet it can provide us a deep comprehension of our complicated environment.

f. Inconsistency

One of the most important aspects of the Internet of Things is its heterogeneity. IoT devices can communicate with other devices or service platforms over various networks, and they are built on various hardware platforms and networks. The four main design criteria for heterogeneous objects in the Internet of Things are extensibility, modularity, scalability, and interoperability. Due to their varied hardware platforms and networks, IoT devices are heterogeneous. They can communicate via various networks with other gadgets or service platforms.

g. Safety

Security risks are inherent to Internet of Things devices. Ignoring security issues with the Internet of Things would be a mistake as we enjoy new experiences, increased efficiency, and other benefits from it. IoT has a lot of privacy concerns and a high degree of transparency. Establishing a security paradigm is necessary in order to safeguard endpoints, networks, and the data that is shared amongst them all.

6. WORKING PROCEDURE OF IOT

IoT works by connecting devices with hardware, such as sensors, that collect data. This data is shared via the cloud and integrated with software, which analyzes and transmits the data to users via an app or website. Smart devices connect to an IoT platform, which is supported by industry giants like Oracle and IBM. The Internet of Things is made possible by technologies that connect devices and enable communication. Connectivity options have pros and cons, with some suitable for smart homes and others for industrial automation. IoT data protocols allow information exchange without an internet connection.

IoT systems are often built using wireless networks, cloud databases for communication, sensors, data processing applications, and intelligent devices that communicate with one another closely. The following elements are used by Internet of Things systems for data processing and exchange:

- ❖ Smart devices that gather, store, and distribute data on other gadgets and parts as well as the surrounding environment. Depending on the objectives of the Internet of Things system, smart devices can be anything from basic sensors to equipment for DNA analysis.
- ❖ Smart devices employ embedded systems, which are made up of different CPUs, sensors, and communication gear. These systems' primary objectives are to gather, transmit, and act upon the data they obtain from their surroundings.
- ❖ Data is sent between IoT devices and the cloud via IoT gateways, hubs, or other edge devices.
- ❖ Data centers in the cloud or on-site that use wireless connections to transfer data between distant computers.

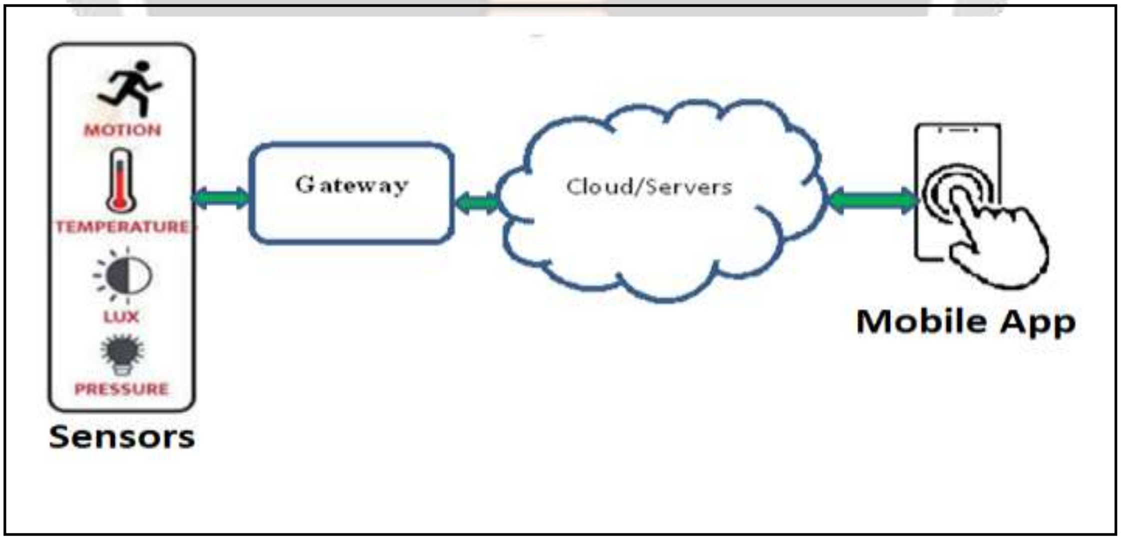

Fig -3: Working Process of IoT

7. TEN COMMON PROTOCOLS FOR IOT COMMUNICATION

Some common protocols for IoT are shown in the following diagram:

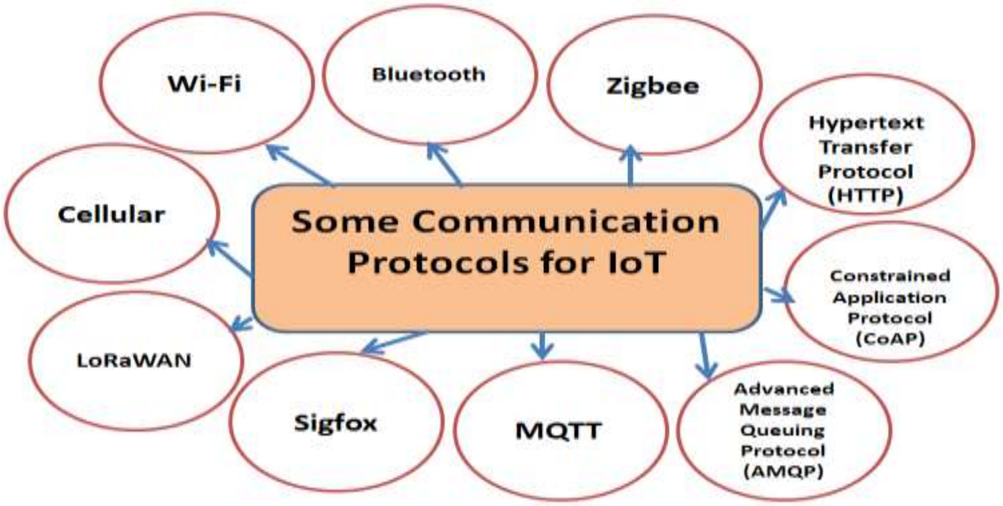
Some Communication Protocols for IoT
Wi-Fi
Bluetooth
Zigbee
Hypertext Transfer Protocol (HTTP)
Cellular
Constrained Application Protocol (CoAP)
LoRaWAN
Sigfox
MQTT
Advanced Message Queuing Protocol (AMQP)

Fig -4: Common Protocols for IoT Communication

8. APPLICATIONS FOR THE INTERNET OF THINGS

Some applications of IoT are:

a. Security systems and thermostats for smart homes
b. Tracking exercise and health with wearable
c. autonomic vehicle diagnostics
d. Smart factory automation
e. Traffic and lighting systems for intelligent cities
f. crop observation
g. Tracking the retail supply chain
h. tracking and identifying illness

9. SECURITY OF IOT

A variety of strategies and tactics are used in Internet of Things security to defend the many technologies, networks, processes, and physical devices that make up an IoT ecosystem against various types of threats. This covers the detection, observation, and reduction of possible device-wide IoT security threats. It is important for the organization to take IoT security seriously for the following reasons:

- Security of data: Legal ramifications and monetary losses may arise from data breaches and leaks.
- Continuity of commercial activities: Problems with IoT security might cause system failures and service outages.
- Trust and reputation: A breach in security has the potential to harm a company's brand and erode customer confidence.

IoT security can be vital to people's lives since certain gadgets are utilized for medical purposes or human protection.

10. IOT SECURITY RISK AND CHALLENGES

Internet of Things (IoT) devices pose several security risks, including weak authentication, low processing power, legacy assets, shared network access, inconsistent security standards, lack of encryption, missing firmware updates, gaps between mobile networks and the cloud, limited device management, and physical vulnerabilities.

- ❖ Weak authentication is a significant concern in IoT security, as default passwords are often weak and can be easily accessed by hackers. Low processing power can make IoT applications difficult to update over-the-air (OTA), making them more vulnerable to hacking. Legacy assets may not be compatible with newer encryption standards, making it difficult to make outdated applications Internet-enabled without significant changes.[4]
- ❖ Shared network access makes the entire network more vulnerable, as hackers can hack an IoT device to gain access to sensitive data or other connected devices. Every IoT application should use a separate network or have a security gateway or firewall to isolate devices from external threats.
- ❖ Inconsistent security standards within IoT make it harder to secure devices and enable machine-to-machine communication without increasing risk. Lack of encryption on regular transmissions is another major threat. Misplaced firmware updates can also pose security risks, as devices can be compromised in the field.
- ❖ Gaps between mobile networks and the cloud can compromise entire IoT deployments. Limited device management can lead to unauthorized access, and end users should be able to detect anomalous behavior and remotely deactivate compromised devices before they cause greater harm.

IoT security risks remain significant, and it is crucial for manufacturers and end users to consider ways to harden devices with better components and security features.

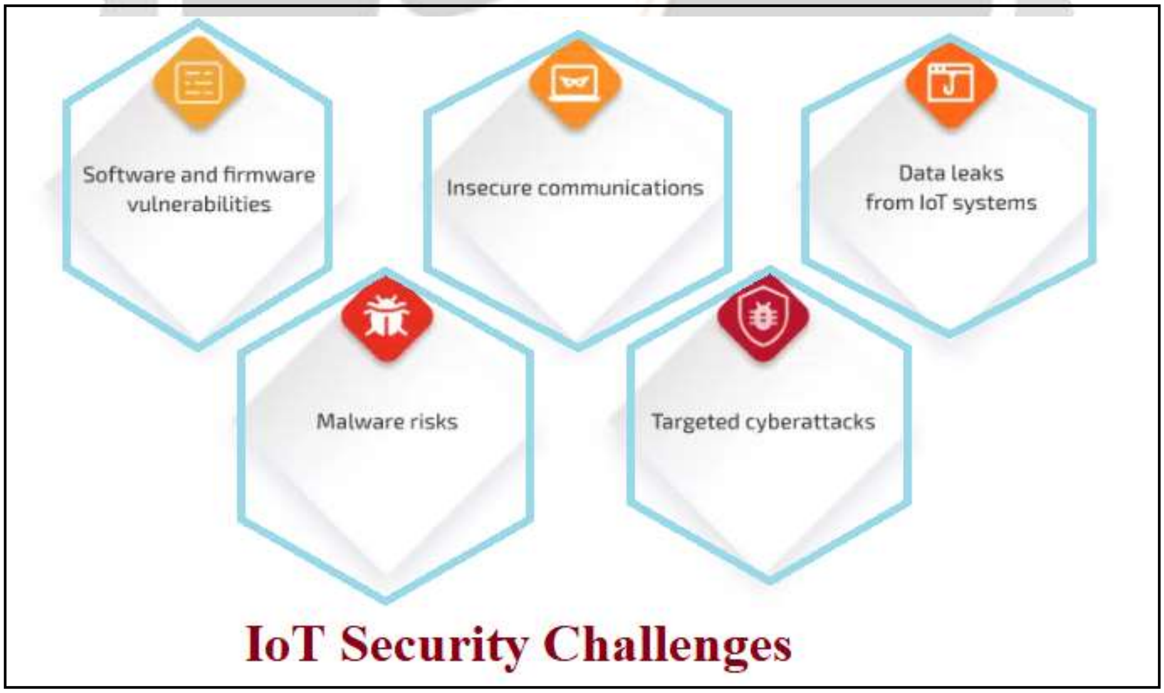

Fig -5: Challenges of IoT Security

11. IOT SECURITY SOLUTIONS

IoT security solutions are crucial for businesses and vendors deploying M2M devices due to the increasing global deployments.

- ❖ Physical security is essential for preventing unauthorized access to devices, and resilient components and specialized hardware are essential.[5]
- ❖ eSIMs are soldered directly onto the circuit board, making them harder to physically access and more resistant to changes in temperature and shock damage.
- ❖ A robust remote-access security protocol is needed to lock SIM functionality to specific devices and remotely disable connections in case of a physical security breach.
- ❖ Private networks are essential for sending and receiving messages through remote devices, and helps IoT manufacturers create Virtual Private Networks (VPNs) using OpenVPN.
- ❖ Abnormality detection is essential for evaluating potential breaches or abnormal network activity.
- ❖ IMEI locks can prevent SIMs from being removed and used in other devices.
- ❖ Encrypted data transfer is necessary for securely transporting data to and from devices, and network-based firewalls protect data from malicious traffic entering the network. Isolating device network connectivity to its core functions is also crucial for security. [6]
- ❖ Both enterprises and device manufacturers are responsible for providing security at the production level.

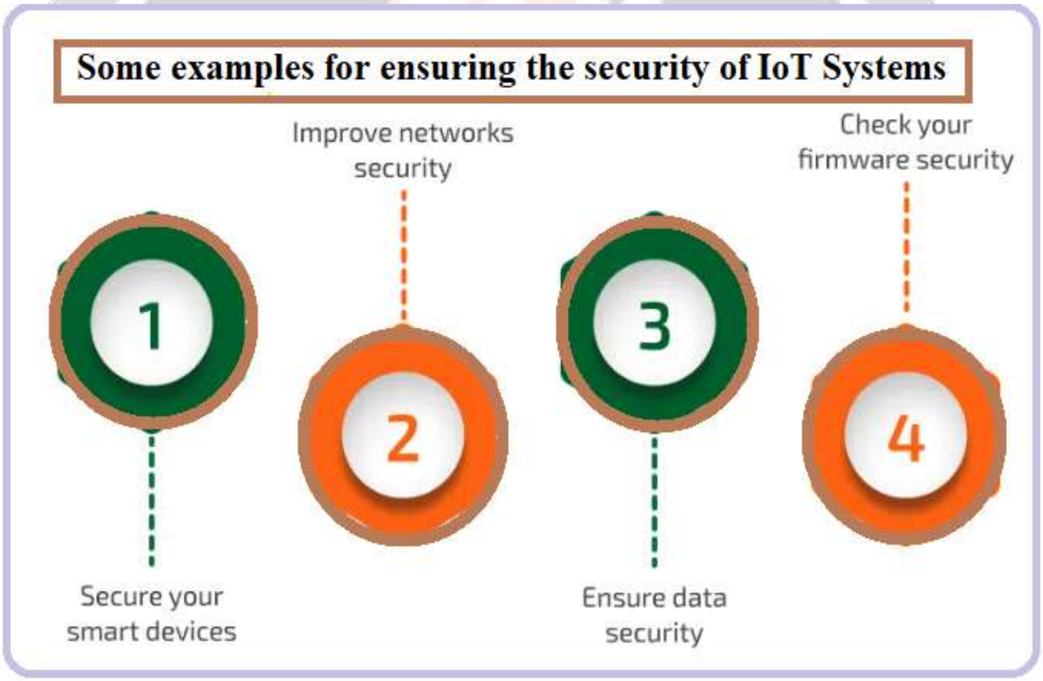
Some examples for ensuring the security of IoT Systems
Improve networks security
Check your firmware security
1
2
3
4
Secure your smart devices
Ensure data security

Fig -6: Some examples for ensuring IoT Systems

12. CONCLUSION

Having covered every angle related to technology, we can conclude that the Internet of Things will dominate the technological landscape for many years to come. IoT's innovative goal of connecting everything to a network would greatly ease people's lives. Its breadth is limitless, and it can constantly adjust to changing circumstances by changing itself. IoT technology is still in its infancy and will advance significantly in the years to come as more study is done in this area. It's clear that the scene is prepared for IoT to embrace everything that comes its way based on how individuals, corporations, and other stakeholders are using IoT in their enterprises. Here, we have enumerated every potential and existing use case for IoT, along with some real-world advice from eminent academics and problems that may arise. For anybody interested in the field of Internet of Things research, this article can serve as a thorough and broad resource.

REFERENCES

[1]. https://www.google.com
[2]. https://www.wikipedia.org/.com
[3]. G.Mahalakshmi, M.Vigneshwaran, "IOT Based Home Automation Using Arduino", International Journal of Engineering and Advanced Research Technology (IJEART) ISSN: 2454-9290, Volume-3, Issue-8, August 2017
[4]. AbdelRahman H. Hussein, "Internet of Things (IOT): Research Challenges and Future Applications",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 6, 2019
[5]. Sunilkumar Malge, Pallavi Singh, "Internet of Things (IoT): Security Perspective", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

BIOGRAPHIES

	Rafat Ara teaches as an Assistant Professor in the German University Bangladesh's Department of Computer Science and Engineering in Gazipur, Bangladesh. She graduated with a B.Sc. in computer science and engineering from Jatiya Kabi Kazi Nazrul Islam University (JKKNIU) in Bangladesh and an M.Sc. in computer science from Jahangirnagar University (JU) in Bangladesh. Her research interests include cloud computing, artificial intelligence, computer networks, Internet of Things, software engineering, cryptography, and network security. She has published research papers in a number of national and international journals.
	Md. Abdur Rahim teaches as an Assistant Professor at German University Bangladesh in Gazipur, Bangladesh, in the Department of Computer Science and Engineering. He received his M.Sc. in computer science from Jahangirnagar University (JU), Bangladesh, and his B.Sc. in computer science and engineering from Jatiya Kabi Kazi Nazrul Islam University (JKKNIU), Trishal, Mymensingh, Bangladesh. He has authored numerous research articles for both domestic and foreign publications. Software engineering, cloud computing, Internet of Things, blockchain technology, internet and web programming, and wireless communications are some of his areas of interest in research.