iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.54409

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 11 Issue VI Jun 2023- Available at www.ijraset.com

Current Trends and Challenges of IOT Next 5 Years

Mrs. Siddalingamma
Residential Govt. First Grade Degree College Mudnal , Dist, Yadgiri

Abstract: ***The world is moving forward at smart , and the credit goes to ever growing technology. One such concept is IOT (Internet of things) with which automation is no longer a virtual reality. IOT connects various physical objects through the internet and enables them to share information with their community network to automate processes for humans and makes their lives easier and confortable . The paper presents the current trends and future challenges of IoT next 5 years , such as the technical, business and legal challenges.***

Keywords: IoT, Internet of Things, challenges, trends

I. INTRODUCTION

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. As it demands communication between objects, everybody should be able to fetch any content from any device at any point of time from anyone located anywhere and who is a part of any business or service, through any path or network. Constructively, availability is a critical factor that affects the performance of IOT [3].The Internet of Things, or "IoT" for short, is about extending the power of the internet beyond computers and smartphones to a whole range of other things, processes and environments.

As the Internet of Things (IoT) continues to steer operations in the 21st century, numerous challenges are coming to light. While the IoT still has the potential to transform business for owners, employees and customers alike, those who already embrace this next-gen network still have some work to do.Not only are they trying to make the most of IoT integration to benefit their own company, but they're also treading new ground and serving as role models for those who have yet to take the plunge.

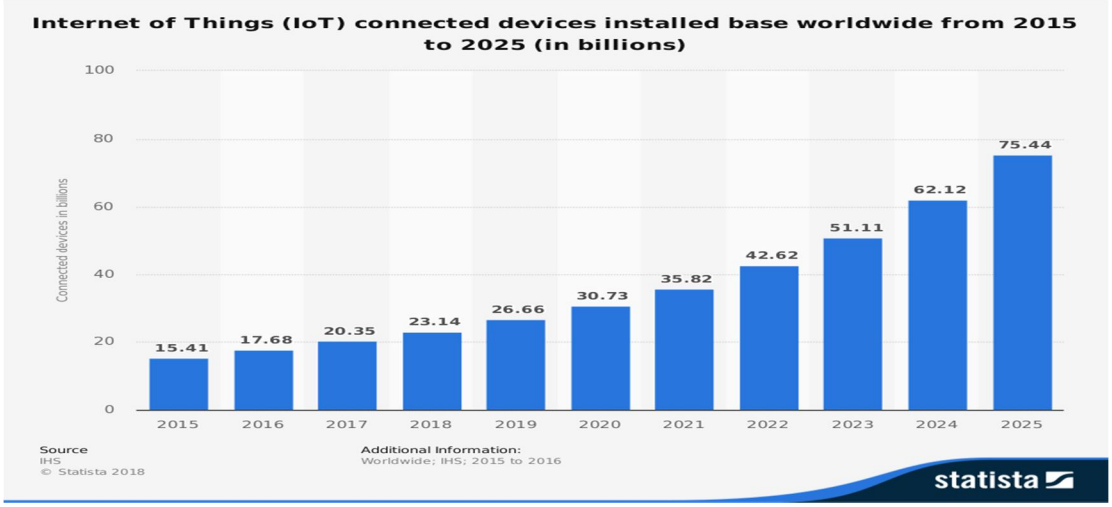
Fig 1.Definition of internet of things next five years

II. PAST AND FUTURE GROWTH OF INTERNET

The number of the Internet of Things is forecasted to grow to 30 billion devices by 2020 and the number is believed to reach approximately 75 billion by 2025. The number of devices connected to the Internet, including the machines, sensors, and cameras that make up the Internet of Things (IoT), continues to grow at a steady pace.

A new forecast from International Data Corporation (IDC)estimates that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025. IDC also projects that the amount of data created by these connected IoT devices will see a Compound Annual Growth Rate (CAGR) of 28.7% over the 2018-2025 forecast period.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com



III. THE TOP 10 CURRENT TRENDS OF IOT

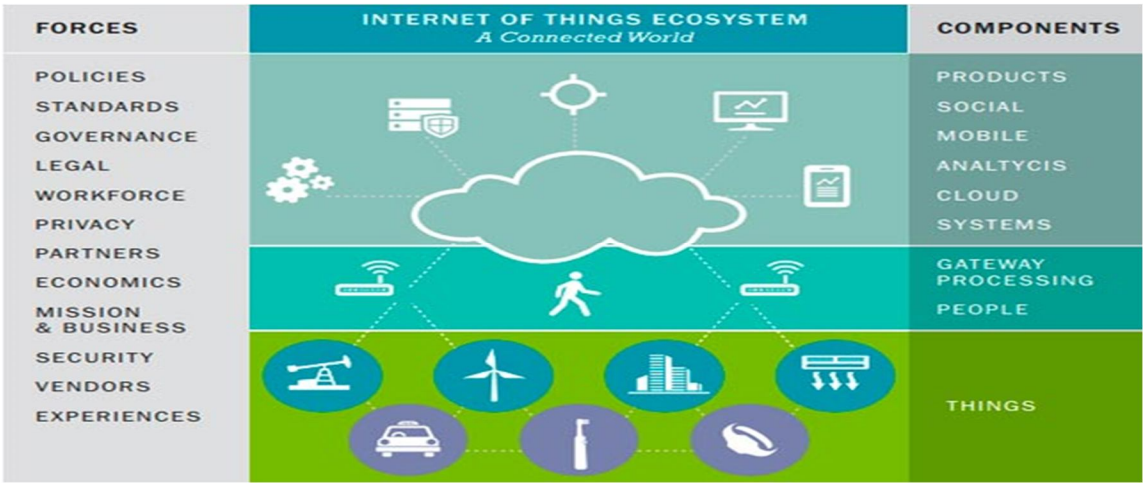
The main purpose of IoT in the workplace is to make the lives of workers more convenient and efficient. Artificial intelligence and advanced analytics can help create a more intelligent work environment.

A. Platforms

The platform is the key to success. The "things" will get increasingly inexpensive, applications will multiply, and connectivity will cost pennies. Keeping in mind that IoT platforms bundle many of the infrastructure components of an IoT system into a single product. The services provided by such platforms fall into three main categories:

1) Low-level device control and operations such as communications, device monitoring and management, security, and firmware updates.
2) IoT data acquisition, transformation and management.
3) IoT application development, including event-driven logic, application programming, visualization, analytics and adapters to connect to enterprise systems.

B. Standards and Ecosystems



Gartner noted that as IoT devices proliferate, new ecosystems will emerge, and there will be "commercial and technical battles between these ecosystems" that "will dominate areas such as the smart home, the smart city and healthcare. Organizations creating products may have to develop variants to support multiple standards or ecosystems and be prepared to update products during their life span as the standards evolve and new standards and related APIs emerge," according to Gartner.

There will be a battle for IoT application mindshare. With billions of devices projected to be spewing out petabytes of data, application developers will have a field day launching thousands, or even millions, of new and cool apps. But, similar to the smartphone world, all of these apps will be fighting for mindshare, and only a few will rise to the top to be valued by businesses and consumers.

C. Event Stream Processing

According to Gartner: "Some IoT applications will generate extremely high data rates that must be analyzed in real time. Systems creating tens of thousands of events per second are common, and millions of events per second can occur in some telecom and telemetry situations. To address such requirements, **distributed stream computing platforms (DSCPs) have emerged**. They typically use parallel architectures to process very high-rate data streams to perform tasks such as real-time analytics and pattern identification."

D. Operating Systems

There's a wide range of systems out there that have been designed for specific purposes.

E. Processors and Architecture

Designing devices with an understanding of those devices' needs will require "deep technical skills."

F. Low-Power, Wide-Area Networks

Current solutions are proprietary, but standards will come to dominate. According to Gartner: "Traditional cellular networks don't deliver a good combination of technical features and operational cost for those IoT applications that need wide-area coverage combined with relatively low bandwidth, good battery life, low hardware and operating cost, and high connection density. The long-term goal of a wide-area IoT network is to deliver data rates from hundreds of bits per second (bps) to tens of kilobits per second (Kbps) with nationwide coverage, a battery life of up to 10 years, an endpoint hardware cost of around $5, and support for hundreds of thousands of devices connected to a base station or its equivalent. The first low-power wide-area networks (LPWANs) were based on proprietary technologies, but in the long term emerging standards such as Narrowband IoT (NB-IoT) will likely dominate this space."

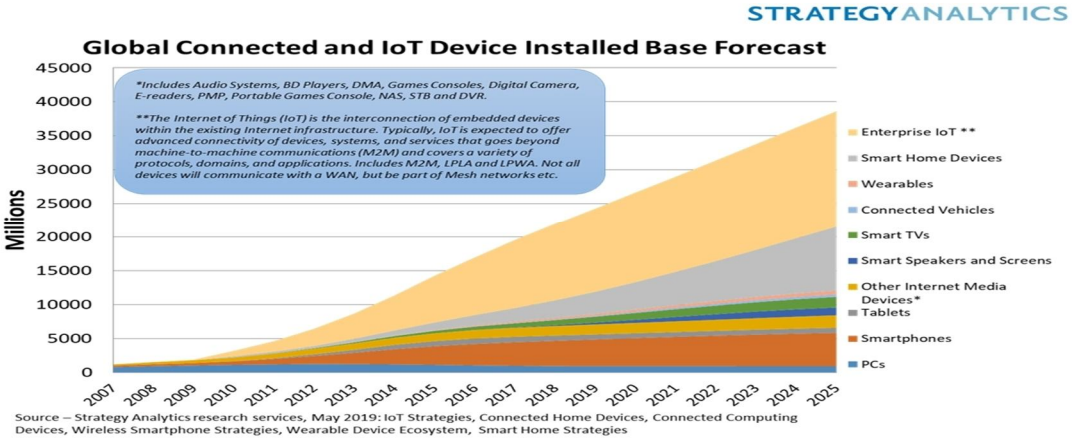
G. Low-Power, Short-Range IoT Networks

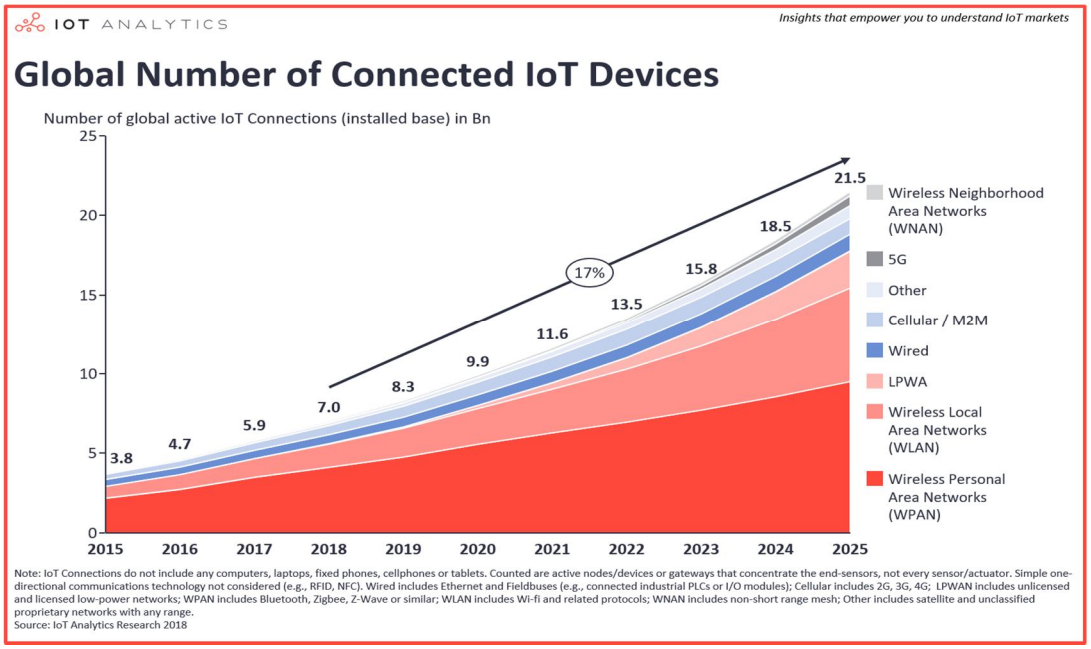
Short-range networks connecting IT devices will be convoluted. There will not be a single common infrastructure connecting devices.

H. Device (Thing) Management

IoT things that are not ephemeral — that will be around for a while — will require management like every other device (firmware updates, software updates, etc.), and that introduces problems of scale.

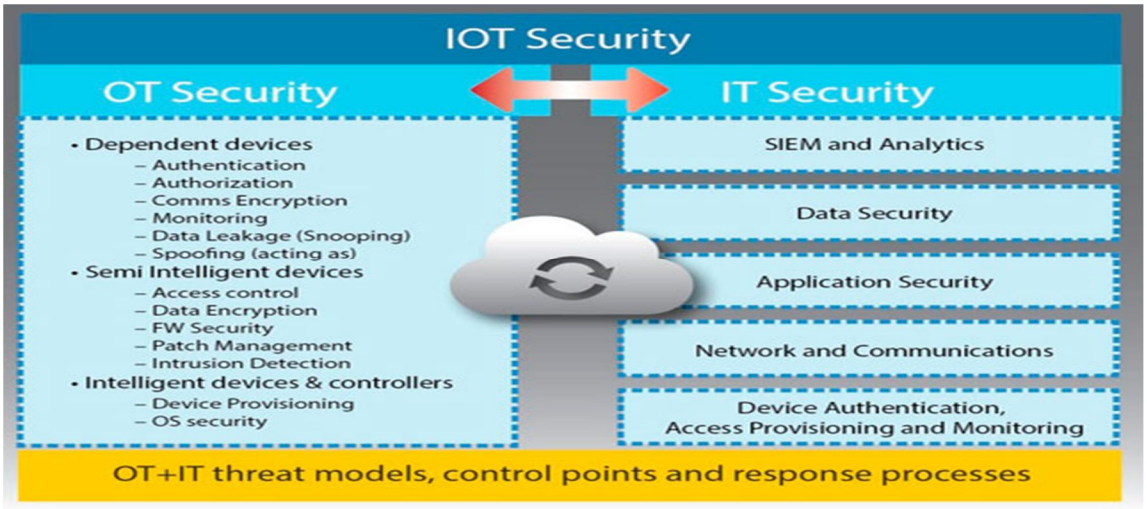
I. Analytics





According to Gartner, IoT will require a new approach to analytics. “New analytic tools and algorithms are needed now, but as data volumes increase through 2021, the needs of the IoT may diverge further from traditional analytics,” according to Gartner. The currency of IoT will be “data.” But, this new currency only has value if the masses of data can be translated into insights and information which can be converted into concrete actions that will transform businesses, change people’s lives, and effect social change.

J. Security



According to Gartner, threats extend well beyond denial of sleep attacks: Those are attacks using malicious code, propagated through the Internet of Things, aimed at draining the batteries of your devices by keeping them awake. According to Gartner “The IoT introduces a wide range of new security risks and challenges to the IoT devices themselves, their platforms and operating systems, their communications, and even the systems to which they’re connected. Security technologies will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as impersonating ‘things’ or denial-of-sleep attacks that drain batteries. IoT security will be complicated by the fact that many ‘things’ use simple processors and operating systems that may not support sophisticated security approaches.”

IV. CHALLENGES IN IOT

1) People will get addicted to Tech connections
2) Say no to Unplugging!
3) Increase in Internet participants
4) Risk mitigation and Human ability will make IoT safer

A. *Meeting Customer Expectations*

In the 1990s, the widespread availability of internet access forever changed the way consumers shop. It also switched the customer's focus from standardized, mass-produced goods to customized products and services.

With the year 2020 on the horizon, customers have higher expectations than ever before. According to a recent report by Salesforce, 57 percent of consumers are more interested in doing business with an innovative or forward-thinking company — and 50 percent won't hesitate to switch brands if their needs go unmet.

B. *Easing Security Concerns*

The IoT was initially touted as a hyper-secure network that was suitable for storing and transmitting confidential datasets. Although it's true that the IoT is more secure than the average internet or LAN connection, it's not exactly the bulletproof shell some users expected.

Some of the most significant security concerns involve both the IoT and the cloud. A recent analysis predicts a loss of up to $120 billion in economic fallout in the takedown of just one cloud datacenter.

Reports also state an annual economic cost of cybercrime at upward of $1 trillion — which is quite a leap for 2017's record-setting figure of roughly $300 billion.

C. *Keeping IOT Hardware Updated*

Regardless of how a company uses the IoT or the cloud, data integrity is a common challenge. With so much data coming in from multiple sources, it's tough to separate useful, actionable information from irrelevant chatter.

It's critical to calibrate your IoT sensors on a regular basis, just as you would any other kind of electrical sensor. Next-gen sensors are embedded in many different devices, including panel meters, chart recorders, current clamps, power monitors and more, and it's difficult to synchronize the dataflow between all this hardware without the help of a professional team.

D. *Overcoming Connectivity Issues*

In its current form, the IoT utilizes a centralized, server-client model to provide connectivity to the various servers, workstations and systems. This is quite efficient for now, since the IoT is still in its infancy, but what happens when hundreds of billions of devices are all using the network simultaneously?

According to updated reports from Gartner, more than 20 billion individual units will connect to the IoT by 2020. It's just a matter of time before users start to experience significant bottlenecks in IoT connectivity, efficiency and overall performance.

E. *Waiting For Governmental Regulation*

While some businesses immediately embraced the IoT, others are hesitant. In many cases, these businesses are waiting for government officials to intervene with new standards and regulations.

However, since the IoT, the cloud and even the common Internet aren't tied to one specific city, state or region, who is responsible for setting these regulations?

Complicating matters even further is the sheer amount of IoT-connected devices. Since these devices originate from many different sources, including international partners and vendors, how does a localized regulatory agency control the quality of incoming shipments?

Although most experts agree that IoT regulation is a necessity, they have yet to formulate any standards or guidelines for the public to follow.

F. *Security Challenges*

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world.

The hacking of baby monitors, smart fridges, Barbie dolls, drug infusion pumps, cameras and even assault rifles are portending a security nightmare being caused by the future of IoT. So many new nodes being added to networks and the internet will provide malicious actors with innumerable attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from security holes.

The more important shift in security will come from the fact that IoT will become more ingrained in our lives. Concerns will no longer be limited to the protection of sensitive information and assets. Our very lives and health can become the target of IoT hack attacks, as was shown in the hacking of pacemakers. Critical city infrastructure can also become a target, as the Ukraine power grid hack warned us last year.

There are many reasons behind the state of insecurity in IoT. Some of it has to do with the industry being in its "gold rush" state, where every vendor is hastily seeking to dish out the next innovative connected gadget before competitors do. Under such circumstances, functionality becomes the main focus and security takes a back seat.

Also, many IoT developers often come from an embedded systems programming background and are ignorant of the threats of IoT programming. They don't necessarily have the knowhow and expertise to program for the hostile connected environment of the internet, and end up dishing out code that is reliable from a functionality perspective, but can easily be exploited remotely.

Scalability issues also contribute to the creation insecure IoT products. The fact is that many security solutions being used today have been created with generic computing devices in mind. IoT devices often lack the computational power, storage capacity and even proper operating system to be able to deploy such solutions.

G. Privacy Challenges

Some of the data that IoT devices collect are very sensitive and are protected by legislations such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and are fundamentally different from our browsing and clicking habits. Yet the necessary precautions aren't taken when storing the data or sharing it with other service providers. Vendors and manufacturers must either discard this data or remove the Personally Identifiable Information (PII) to make sure that consumers aren't damaged in case of data breaches.

Another consideration to take is that while data generated about a single appliance (such as a smart toaster) might not be sensitive per-se, yet when combined with data from other devices, it can reveal information such as the consumer's life pattern, which can become very damaging if they fall into the hands of the wrong people. In many cases, criminals don't even need to pry into your encrypted communications in order to obtain the information they want. A study by LGS Innovations elaborates on this issue and presents a DiY solution to protect IoT traffic and privacy.

H. Compatibility and Longevity Challenges

As an industry that is going through its baby steps, IoT is growing in many different directions, with many different technologies competing to become the standard. For instance, we currently have ZigBee, Z-Wave, Wi-Fi, Bluetooth and Bluetooth Low Energy (BTLE) all vying to become the dominant transport mechanism between devices and hubs. This will cause difficulties and require the deployment of extra hardware and software when connecting devices.

Other compatibility issues stem from non-unified cloud services, lack of standardized M2M protocols and diversities in firmware and operating systems among IoT devices.

Rendering the devices implementing them useless. This is especially important, since in contrast to generic computing devices which have a lifespan of a few years, IoT appliances (such as smart fridges or TVs) tend to remain in service for much longer, and should be able to function even if their manufacturer goes out of service.

I. RiskIncrease

Whether the people are connected or not but the chance will stay, with the massive increase in the IoT devices usage. This may lead to security and liberty issues getting magnified by the IoT devices.

The Threats can turn into gruesome attacks and all the other acts which can be very violent. The physical attacks are in the public and people can watch it. However in the cyber attacks will be in private and you will not know who is the attacker but the results are terrible.

With the rise of the IoT and the security, the concern will increase so as the liberties by the users. You can say this will help to know where you are walking and light your way or can grab your sensitive and personal information. It will become the biggest challenge for the cops, government and the whole world.

J. Lack Of Experience Challenges

Manufacturing organizations are not in the business of cybersecurity. As such, they are unknowingly making it easier for cybercriminals to breach a network. We saw this first with the PC industry. PCs have been manufactured by engineers that are experienced in hardware and software development for over 25 years, and while they might be attempting to build them with proper security, they have ultimately been unsuccessful. But now, businesses operate in digital and physical environments that continue to grow as new technologies, including IoT, are added to the network. As a result, the complexity of the environment increases. So, IoT manufacturers face the same challenge PC manufacturers did — they might attempt to make their devices secure, but since this is not their area of expertise, they are failing to do so.

V. MOTIVATION

IoT has become one of the most significant elements of the future Internet with a huge impact on social life and business environments. IoT current trends with future Challenges of next 5 years are more clearly discussed above . To secure IoT against those challenges, a secured technology is needed in these application areas.The main motivation behind this detailed study is IoT trends leads challenges.

VI. WHAT IS NEXT?

The market is endless. The future of IoT looks bright and promising. With all the predictions and concepts in the works, our lives are about to turn much easier and efficient whether we are talking about navigating around our cities, interacting at work or lodging in the comfort of our own homes. However, there's one constraint IoT devices face in all these sectors — the problem of connectivity and communication between all the devices. It's exciting but you need to build great software and hardware with a sophisticated backend with multiple security levels and to bring order and sophistication to data and understanding that security is an art that involves cryptography. Most companies don't have the talent they need to develop secure products.If companies manage to overcome this obstacle, the way we live now will be an ancient past.

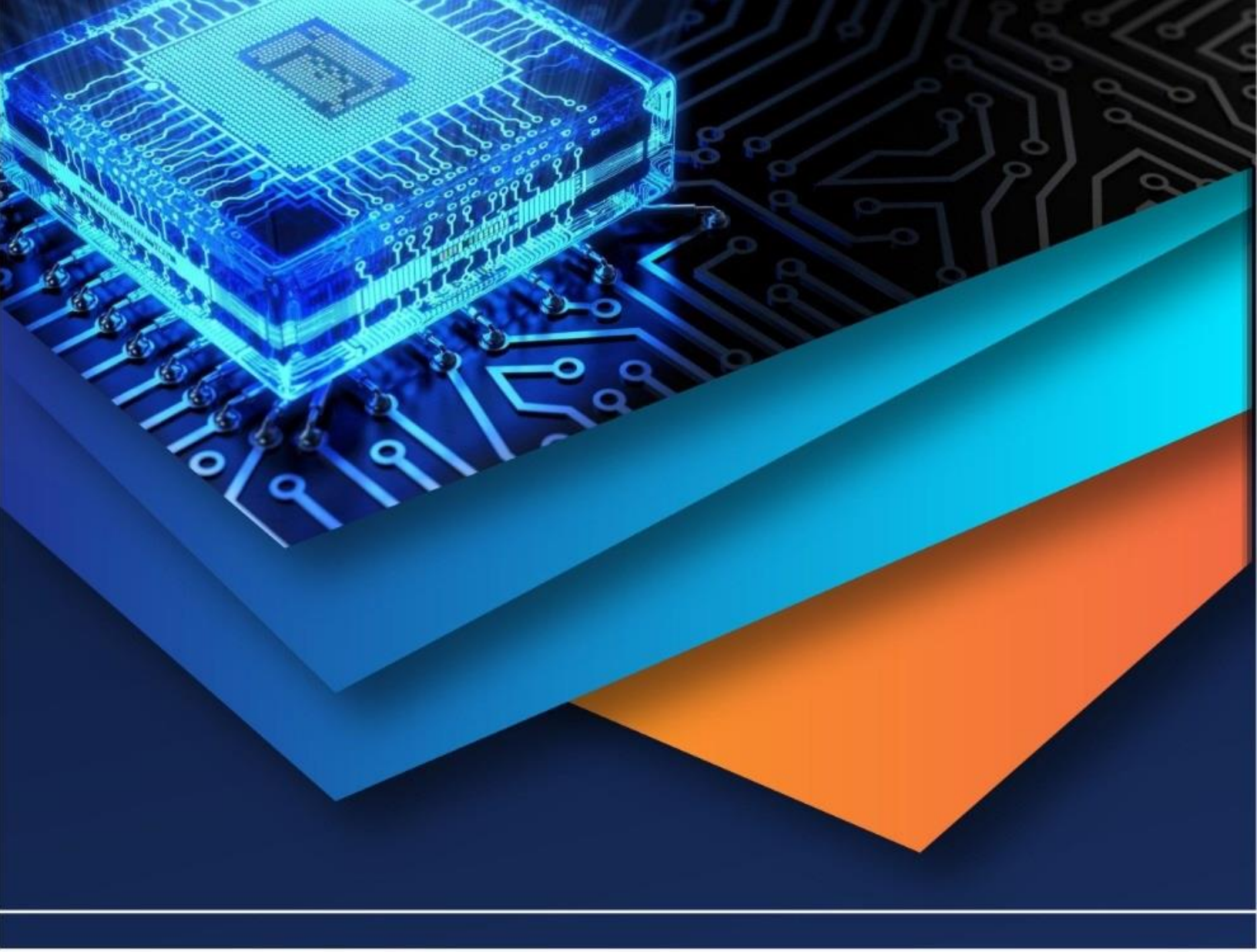
VII. CONCLUSION

We come to an end that the IoT or the internet of things has made the lives of the human being smart and comfortable. It has made the lives of the people very convenient. The Internet of Things continues its brisk and steady rise, and many trends that started in previous years will continue or even accelerate for the foreseeable future. Where as on the other hand with the increased use of the internet of things the treat for security and safety has also increase. So we should be careful while providing the details on the internet platform.

REFERENCES

[1] Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X). Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. Journal of Network and ComputerApplications, 36(6), 1531-1539.
[2] Triantafyllou, A., Sarigiannidis, P., &Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. Wireless communications and mobile computing, 2018.
[3] Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1577-1581). IEEE.
[4] Yeo, K. S., Chian, M. C., & Ng, T. C. W. (2014, December). Internet of Things: Trends, challenges and applications. In 2014 International Symposium on Integrated Circuits (ISIC) (pp. 568-571). IEEE.
[5] Keramidas, G., Voros, N., &Hübner, M. (2016). Components and Services for IoT Platforms. Springer International Pu.
[6] https://www.bbvaopenmind.com/en/technology/digital-world/10-predictions-for-the-future-of-iot/
[7] http://www.dbta.com/BigDataQuarterly/Articles/10-Predictions-for-the-Future-of-IoT-109996.aspx

[8] https://campustechnology.com/articles/2016/02/25/security-tops-list-of-trends-that-will-impact-the-internet-of-things.aspx
[9] https://www.softscripts.net/blog/2019/01/future-of-iot/4 Major Technical Challenges Facing IoT Developer ,4 Major Technical Challenges Facing IoT Developers



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY