iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49873

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 III Mar 2023- Available at www.ijraset.com

Network Security Key Areas of IoT and IIOT- with Connected Devices Privacy and Security

Dharavath kotaiah[1], Chitti Ravi Kiran[2]
[1]*Assistant Professor (PT),Department of Mining Engineering, University College of Engineering, Kakatiya University, Kothagudem, Telangana, India*
[2]*Lecturer,Department of Mining Engineering, University College of Engineering, Kakatiya University, Kothagudem, Telangana, India*

Abstract: ***With the accelerating pace of technological advancement, demand for IoT app development is at an all-time high. Statistic predicts that $1.1 trillion will be spent globally on IoT. (approx.).Modern IoT apps and solutions will unquestionably become more popular as a result of this. Who will get the newest item into consumers' hands first among manufacturers is still a point of contention. Companies can profit much from IoT app development, but one of the key considerations is security. This post focused on IoT security issues and solutions. IoT solutions can be implemented by businesses of any size and in any industry to boost productivity and customer satisfaction. This article all about the security of IoT and IIoT how to overcome them. Organizations regardless of industry and size can make IoT solutions a part of their business to increase customer satisfaction and efficiency.***
Keywords: IoT, IIoT, Security, Communication, Encryption, Vulnerable interfaces.

I. INTRODUCTION

A. *IIoT and Network Security Standard*

Universal IoT/IIoT standards are being developed by a number of network security standards groups, including those driven by tech behemoths like Google, Intel, Coal India, Vedanta Recourses and Qualcomm. None of these groupings has emerged despite ongoing discussions about IoT design, interoperability, privacy, and security. Like the epic fight between Betamax and VHS, may the best concepts prevail. The majority of nations have been striving to create their own IoT/IIoT standards, although there are several approaches to doing so.

In the globe today, there are about 23 billion connected IoT devices. By the end of 2025, this number will have increased to 60 billion people. This huge influx of new technology has a price. Few of them take into account the security concerns related to data access & management as well as the IoT devices themselves. What are the biggest security and privacy issues affecting IoT-connected devices right now? The fact that IT corporations are too reckless when it comes to handling device-related security concerns is actually one of the key issues with the companies producing these gadgets. The majority of these IoT products and gadgets receive insufficient upgrades, and others never receive crucial security fixes.

B. *Key Areas of Devices Privacy and Security*

1) A lack of testing and upgrading
2) The use of default passwords and brute-forcing
3) Lack of IoT expertise
4) IoT device management issues
5) Malware for IoT and ransomware
6) Crypto currency-focused IoT botnets
7) Concerns about data security and privacy
8) Device Update Management Security Issues
9) a lack of adequate data protection
10) Vulnerable interfaces
11) Using malicious IoT devices
12) Security Hazards of IoT

13) IoT threats that are subtle and undetectable
14) Robotics and AI
15) Domestic Invasion
16) remote access for vehicles
17) Unreliable communication
18) Managing IoT security risks effectively

C. A lack of testing and upgrading

This implies that a device, which the users first believed to be secure, later becomes insecure and vulnerable to hackers and other security issues. The same issue existed in early computer systems, and automatic updates helped to some extent. Yet, IoT manufacturers are more eager to create and deploy their products as soon as possible, without giving security much of a thought. However, most manufacturers only provide firmware updates for a little amount of time before stopping as soon as they begin developing the following attention-grabbing device. Even worse, they make use of outdated, unsupported Linux kernels. Due to obsolete technology and software, this exposes their loyal customers to future attacks.

D. The use of default passwords and brute-forcing

One of the finest instances of the problems associated with sending devices with default passwords and failing to advise customers to change them as soon as they receive them is the Mirai botnet, which has been utilised in some of the biggest and most disruptive DDoS attacks. Some government studies caution manufacturers against marketing IoT devices that have weak security settings, like employing the username and/or password "admin."That said, these are merely guidelines at this point, and there are no legal penalties to encourage manufacturers to stop using this risky method. Nearly all IoT devices are vulnerable to password cracking and brute-forcing in particular, due to weak passwords and login information. The fact that Mirai malware found susceptible IoT devices and used their default passwords to log in and infect them is the sole explanation for its success. Therefore, any business that used factory default credentials on their devices put their assets, their customers' valuable information, and their business at risk of being the target of a brute-force attack.

E. Lack of IoT expertise

Many businesses have stated that there is now a significant talent gap among IoT security professionals. Companies are unable to fully utilise employee potential due to the skill gap.

F. IoT device management issues

Devices in the healthcare, retail, manufacturing, and life sciences that are IoT and IoMT (Internet of Medical Things) enabled. It exposes numerous flaws in a remarkably varied collection of related things. The biggest causes of IoT device security vulnerabilities are computed tomography and magnetic resonance imaging equipment. Traditional connected gadgets and outdated systems, like ventilators, patient monitors, lights, infusion pumps, and thermostats, are vulnerable to hacking attempts that include:

1) Operations disruption,
2) Consumer data and safety breaches,
3) Financial setbacks,
4) A reputational hit.

G. Malware for IoT and ransomware

In the next years, as the number of IoT-connected devices increases, so will the amount of malware and ransomware that target them. A growing number of malware and ransomware strains are attempting to combine the various modes of attack, whereas classic ransomware depends on encryption to totally lock out users from various devices and platforms. Potentially, ransomware attacks would concentrate on stealing user data while restricting and/or disabling device operation.

H. Crypto currency-focused IoT botnets

Hackers looking to profit from the crypto currency boom are finding the fierce mining competition and recent spike in bit coin valuations to be too alluring. Although most people consider block chain to be hacker-resistant, there seem to be more attacks in the block chain industry lately. Instead of the block chain itself being vulnerable, it is the block chain app development that uses it.

In order to obtain usernames, passwords, and private keys, social engineering is being utilised. Nevertheless, it will be used more frequently in the future to compromise block chain-based applications. One of the numerous digital currencies that are now mined with IoT devices is the open-source coin Monero.Some hackers have even turned IP and video cameras into crypto currency mining devices. Data integrity manipulation, IoT botnet mining, and block chain breaches all greatly increase the potential of flooding the open crypto currency market and upsetting the already unstable value and structure of crypto currencies.

I. Concerns About Data Security and Privacy

In today's linked society, data privacy and security continue to be the top concerns. Large businesses continually collect, transmit, store, and process data using a wide range of IoT devices, including linked printers, HVAC systems, smart thermostats, speakers, and lighting systems. All of this user data is frequently shared between or even sold to different businesses, which violates our rights to privacy and data security and increases public mistrust.

J. Device Update Management Security Issues

One of the biggest factors affecting software security is firmware or software. A producer, however, can include the most recent product updates with the gadgets he sells. These changes have the potential to lead to some security issues.

K. A lack of adequate data protection

One of the most important IoT security issues can be a lack of adequate data protection. Hazardous communications or data storage may trigger this problem. The ability of compromised devices to access private information is one of the key weaknesses in IoT security. It is now more important than ever to separate networks and store data securely.

L. Vulnerable Interfaces

Data is processed and communicated by every IoT device. For communication, they require apps, services, and protocols, and many IoT security fixes come from unsecure interfaces. Some of the most frequent interface problems are a lack of adequate device authentication, inadequate encryption, or no encryption at all.

M. Using malicious IoT devices

One of the most destructive types of malware is ransomware. With encryption, it prevents access to your sensitive files. The scammer will then demand a ransom payment to unlock the sensitive material. Future wearable's, smart homes, medical technology, and other ecosystems may be in danger.

N. Security Hazards of IoT

Devices that can connect to the Internet of Things present their users with a number of security challenges. The basic IoT security vulnerabilities are not particularly new, despite the incredible connectedness that IoT has brought to gadgets. In addition to this, there are a number of negative hazards associated with the Internet of Things, including low processing power, network access sharing, inconsistent security standards, a lack of firmware upgrades, etc.

IoT Threats those are Subtle and Undetectable

The Mirai botnet was the biggest IoT-based botnet. Botnet that was far riskier than the well-known Mirai. Although if large-scale attacks can be crucial we should be worried about the smaller, harder to detect attacks. Over the next couple of years, we can expect to witness an increase in the number of micro-breaches that manage to evade security measures.

O. Robotics and AI

Enterprises will soon have to cope with tens of thousands, if not millions, of IoT devices as they continue to permeate our daily lives. From the standpoint of data collecting and networking, this volume of user-data can be quite challenging to manage. Automation and AI tools are already being used to filter through enormous amounts of data, and they may one day assist network security officers and IoT administrators in enforcing data-specific regulations and identifying aberrant data and traffic patterns. However, using autonomous systems to make decisions that impact millions of functions across massive infrastructures like healthcare, power, and transportation might be too risky, especially given that it only takes a single error in the code or a malfunctioning algorithm to bring down an entire system.

These are but a few of the most important IoT security issues that we will need to take into account while developing an IoT-based application in the upcoming years. As you can see, the majority of them centre on two concerns: preventing attacks on IoT and preventing theft of user data.

P. Domestic Invasion

The possibility of a home invasion is arguably one of the scariest ones that IoT can provide.
Home automation was made possible by the widespread use of IoT devices in companies and homes nowadays.

Q. Remote access for Vehicles

The IoT also poses the threat of car hijacking in addition to house invasion. Thanks to connected IoT devices, smart vehicles are rapidly approaching reality. However, because of its IoT connection, it also carries a higher risk of a vehicle hijack.

R. Unreliable Communication

Many IoT gadgets communicate with the network using unencrypted messages. One of the greatest IoT security issues currently facing the industry is this. It's high time all businesses made sure their cloud services and gadgets had the best possible encryption.

S. Managing IoT Security risks Effectively

Many Internet of Things (IoT) gadgets communicate with the network using unencrypted messages. There are many IoT security issues, but this is one of the worst. It's time for all businesses to make sure that their online services and technology are fully encrypted.

II. SOLUTIONS FOR DEVICES PRIVACY AND SECURITY

A. A lack of Testing and Upgrading

Each device must undergo thorough testing before being made available to the general public and businesses must update them frequently to safeguard their customers against such attacks. Failure to do so is detrimental to businesses and the customers they serve because it only takes one significant data breach to destroy an organisation.

B. The use of Default Passwords and Brute-forcing

It is recommended to use various SSH security features to block access to the route user in order to avoid brute force attacks. Keep your credentials strong. To prevent sensitive privacy problems, use a strong password or captcha. As part of your security strategy, you should also establish a login cap for a particular IP address or range or you can develop custom login URLs.

C. Lack of IoT Expertise

Training and skill-upgrading programmes must be in place for this. Effective workshops, practical newsletters, and bulletins can have a big impact.

D. IoT Device Management Issues

Implementing IoT security solutions can significantly reduce the aforementioned IoT security concerns. They answer to customer demands for end-to-end solutions as well as the crucial device management security issues. These platforms can enhance the firmware update process, reduce security flaws, notify, and report on specific metrics related to IoT assets.

E. Malware for IoT and Ransomware

Enhance the security of mobile banking applications .Once locked, the webcam can be used to send video to a malicious website, where it can be used to harvest sensitive information using a malware access point and then demand ransom in exchange for the device's unlocking and return of the data. Future unpredictability regarding illegal access or theft will result from the exponential growth of IoT devices.

F. Crypto currency-focused IoT botnets

If future crypto currency abuses are to be avoided, block chain-based IoT systems, apps, and structures must be governed, constantly monitored, and updated.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

G. Concerns About Data Security and Privacy

Prior to storing and separating IoT data payloads from information that can be used to personally identify us, we must establish specific compliance and privacy rules that redact and anonymize sensitive data. Then, cached data that is no longer required should be securely disposed of.

The biggest challenge, if the data is stored, is adhering to various legal and regulatory frameworks. The same procedure should be followed when using mobile, web, and cloud-based applications and services to access, manage, and process IoT device data. Read more about how IoT and block chain technology can protect personal data. For small businesses with tight resources, developing secure mobile apps and web-based IoT applications can be rather challenging.

IoT and block chain development help protect personal data. For small businesses with tight resources, developing secure mobile apps and web-based IoT applications can be rather challenging.

As we already indicated, the majority of manufacturers typically concentrate only on launching the app and gadget as soon as possible in order to draw further investment and begin expanding their user base. You might want to think about searching through a directory of mobile and web development companies and finding the best one that can meet all of your security requirements with multi-layered data management unless you want to run the risk of a significant security breach and damage your brand authority and trustworthiness.

H. Device Update Management Security Issues

The device will also send any automated updates back to the cloud as they occur. This will reduce the amount of time the device is offline. In addition, there is a good chance that the hacker will take the private data if the connection is not encrypted or the files are not safe.

I. A lack of Adequate Data protection

You may use the power of encryption to overcome these data protection concerns. Your sensitive data can be protected from unauthorised access and data theft by being encrypted. Data decryption can also assist you in protecting the privacy and confidentiality of data. In addition, cryptography is a powerful tool for blocking eavesdropping and sniffing attacks, which allow hackers to passively read data from industrial control systems that is being delivered or received via a network. Furthermore, Man In The Middle Attacks are typically defended by using cryptography. Attacks called "Man in the Middle" involve hackers inserting new messages inside crucial ones.

J. Vulnerable Interfaces

To prevent unwanted access to a connected device and the data it generates, use device authentication. Use digital certificates to your advantage so that a digital entity can safely send data. Use the precise norms, best practises, and standards that are available from reliable sources.

K. Using Malicious IoT devices

Malware can occasionally disable all of the device's features. Imagine having the thermostat all the way up and being unable to start your car without paying a ransom.

L. Security Hazards of IoT

When it comes to IoT, security is essential. An eSIM can be directly soldered onto circuit boards if you're using a mobile device, which makes it more difficult for burglars to cause any harm.

M. IoT Threats Those are Subtle and Undetectable

Instead of pulling out all the stops, hackers will probably opt for stealthy assaults that are just small enough to let the data leak out rather than just grabbing millions and millions of records all at once.

N. Robotics and AI

Strict legal and regulatory frameworks directed at manufacturers can address both of these issues, and those who violate them will face severe penalties such as job restrictions and significant fines.

O. Domestic Invasion

As your IP address might be used to identify your home address, the security of these IoT devices is a major problem. Hackers may sell this important data to darknet marketplaces that serve as havens for organised crime. Also, there is a chance that IoT devices you utilise for your security systems could be compromised, posing a serious risk to your home.

P. Remote Access for Vehicles

A skilled hacker might take control of your smart automobile by gaining remote access. The fact that anyone could take control of your car and that you might be exposed to deadly crimes makes this a frightening situation.

Q. Unreliable Communication

Use of transport encryption and security protocols like TLS is the best way to deal with this security problem. Using many networks that isolate various devices is another option. You can also use private communication, which guarantees the confidentiality and security of the data transferred.

R. Managing IoT security risks effectively

Integrity
Availability
Confidentiality

Proper security ensures that all three of these security pillars are upheld. Unauthorized data, software, and services can prevent you from implementing all of the recommended security alternatives, such as authentication and device management solutions, with professional expertise, etc.

III. CONCLUSION

IoT app development can be quite advantageous for businesses, but one of the key considerations is security. IoT security issues and solutions. IoT solutions can be implemented into any organisation, regardless of size or industry, to boost productivity and customer satisfaction. According to a recent report, 61% of firms have encountered cyber security problems in their smart factories. After a cyber attack the largest meat producer in the world, JBS S.A, was forced to close all of its American cattle operations. All of the company's beef processing factories had to close, while all other JBS meatpacking plants in the US encountered some amount of disruption. Although the exact number of plants damaged worldwide by the ransomware attack is yet unknown, the possibility of future attacks is already upending agricultural markets and causing worry about attacks on key infrastructure. Construction, energy, manufacturing, agricultural, and mining industries are all undergoing a rapid digital revolution. It indicates that more of the operations that support these industries are being automated, and components that supply the data necessary to boost production and efficiency are becoming internet-connected. Analysts forecast that the numbers of IIoT devices will more than double to 36.8 billion over the following four years. This exposes asset owners and operators to a variety of fresh dangers.

REFERENCES

[1] P. J. Ryan and R. B. Watson, “Research Challenges for the Internet of Things: What Role Can OR Play?,” Systems, vol. 5, no. 1, pp. 1–34,2017.
[2] M. Miraz, M. Ali, P. Excel, and R. Picking, “Internet of Nano-Things,Things and Everything: Future Growth Trends”, Future Internet, vol. 10,no. 8, p. 68, 2018, DOI: 10.3390/fi10080068.
[3] E. Borgia, D.G. Gomes, B.Lagesse. Lea, andD.Puccinelli, “Special issue on" Internet of Things: Research challenges and Solutions”., “Computer Communications, vol.89, no.90,pp.1–4,2016.
[4] K. K. Patel, S. M. Patel, et al., “Internet of things IOT: definition, characteristics, architecture, enabling technologies, application future challenges,” International journal of engineering science and computing: vol.6, no.5, pp.6122–6131,2016.
[5] S. V. Zanjal and G. R. Talmale, “Medicine reminder and monitoring system for secure health using IOT,” Procedia Computer Science, vol.78, pp. 471–476, 2016.
[6] R. Jain, “A Congestion Control System Based on VANET for Small Length Roads”, Annals of Emerging Technologies in Computing (AETiC), vol. 2, no. 1, pp. 17–21, 2018, DOI:10.33166/AETiC.2018.01.003.
[7] S. Soomro, M. H. Miraz, A. Prasanth, M. Abdullah, “Artificial Intelligence Enabled IoT: Traffic Congestion Reduction in Smart Cities,” IET 2018 Smart Cities Symposium, pp. 81– 86,2018,DOI:10.1049/cp.2018.1381.
[8] Mahmud, S. H., Assan, L. and Islam, R. 2018. “Potentials of Internet of Things (IoT) in Malaysian Construction Industry”, Annals of Emerging Technologiesin Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 44-52, Vol. 2, No. 1, International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2018.04.004.

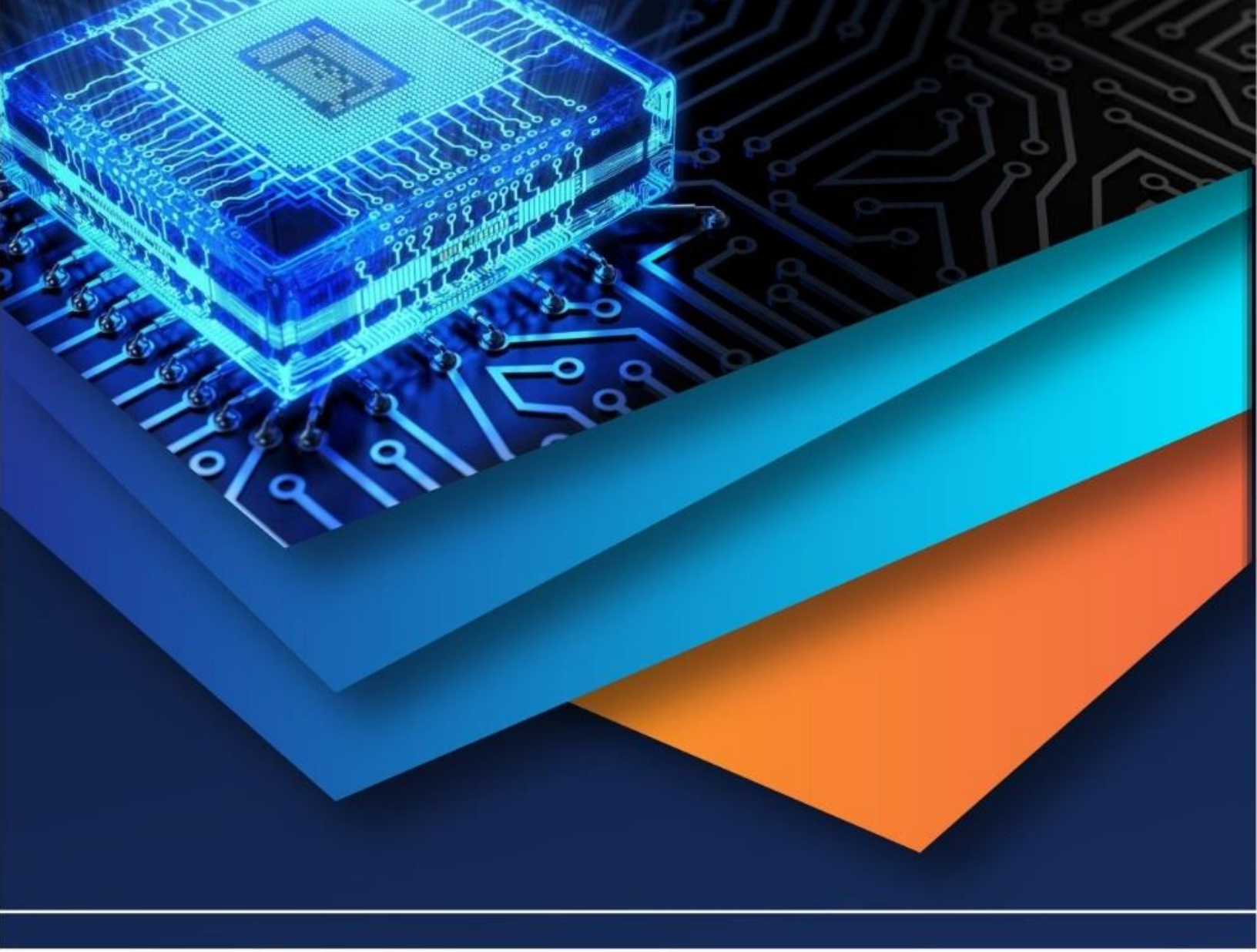
[9] Mano,Y., Faical B. S.,Nakamura L., Gomes, P. G. Libralon, R. Meneguete, G. Filho, G. Giancristofaro, G. Pessin, B. Krishnamachari, and Jo Ueyama. 2015. Exploiting IoT technologies for enhancing Healt Smart Homes through patient identification and emotion recognition.Computer Communications, 89.90, (178-190).DOI:10.1016/j.comcom.2016.03.010.

[10] V. Sundareswaran and M. S. null, "Survey on Smart Agriculture Using IoT," International Journal of Innovative Research in Engineering & Management (IJIREM), vol. 5, no. 2, pp. 62–66, 2018.

[11] P. Tadejko, "Application of Internet of Things in logistics-current challenges," Ekonomia i Zarz{a ,}dzanie, vol. 7, no. 4, pp. 54–64, 2015.

[12] S. Rajguru, S. Kinhekar, and S. Pati, "Analysis of internet of things in a smart environment," International Journal of Enhanced Research in Man-agement and Computer Applications,vol. 4, no. 4, pp. 40–43, 2015.

[13] H. U. Rehman, M. Asif, and M. Ahmad, "Future applications and research challenges of IOT," in 2017 International Conference on Informa-tion and Communication Technologies (ICICT), pp. 68–74, Dec 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY