iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VII Month of publication: July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73318

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Security and Privacy Challenges in IoT: A Review of Threats, Solutions, and Future Trends.

Madhuri R. Mutyal[1], Pallavi Dakhore[2], Bharat Shelke[3]
[1]*Assistant Professor, Department of Management-BCA, Dr.(SOW)I.B.P Mahila kala Mahavidyalaya, Chh. Sambhajinagar*
[2]*Assistant Professor, Department of Computer Application, DITMS College, Chh. Sambhajinagar*
[3]*Associate Professor, Department of Computer science, SCS College, Omerga, Dharashiv*

Abstract: Internet of Things (IoT) has become an innovative technology, which links millions of devices in different spheres, such as healthcare, smart cities, industrial automation, and transport. As much as IoT provides an immense difference in terms of efficiency, Automation and data-driven decision-making, these security and privacy threats are diverse. It's extremely distributed and heterogeneous character, the few resources of a device, and the very high numbers of sensitive data processed by this type of network make IoT systems vulnerable to many threats.

The review gives an in-depth examination of the issues of security and privacy related to IoT. The threats are grouped in five broad categories, which are a device-level, network-level, data-related, cloud/backend, and human/social engineering threats. The existing solutions such as lightweight cryptography, authorization methods, intrusion detection tools, system-based security platforms, and threat-detecting systems based on AI are then evaluated in the paper. Moreover, we examine privacy-protective approaches, including data anonymization, differential privacy, federated learning and secure multi-party computing.

Besides, the paper raises such emerging trends as Zero Trust Architecture, quantum-safe cryptography, and edge computing security along with key open challenges such as standardization, secure updates, and usability. This review will discuss present research on as well as the industry practices to provide guidance on future research that checks wholesome, scalable, privacy-preserving IoT systems.

Keywords: IoT, threats, challenges, future trends etc.

I. INTRODUCTION

The Internet of Things (IoT) is a fast emerging paradigm that links physical objects, such as homes appliances and wearable devices, as well as industrial equipment, office gadgets, and smart city infrastructure to each other over the internet to transmit, share and utilize data. The ecosystem allows real-time decision-making and automation in various industries and segments including healthcare, agriculture, manufacturing, etc. The industry is making projections that the IoT connected devices will exceed 30 billion of connected devices worldwide in the next several years, which only represents a fraction of its potential in transforming operations across industries[1][2]. Even though IoT is a great technology, it brings serious security and privacy challenges. The diversity of threats in IoT systems is possible due to the high degree of distribution of IoT networks, heterogeneity of used devices, and sensitive data processed. IoT is also vulnerable to cyberattacks because of weak authentication, unsecure channels of communication, the absence of standardization across the entire spectrum and restrictions in the computing capabilities of edge devices. In addition to that, privacy breaches on personal, medical, or location data may be dangerous both to the individuals and to the organizations.

The growing number of attacks as well as their complexity against IoT systems have highlighted the importance of effective security and privacy systems. Nevertheless, the deployment of most IoT applications remains burdened by the challenges of providing holistic, large-scale, and efficient utilization of resources. The necessity to generalize the existing information about the current threats and countermeasures represents the driving force of this review, with the aim of influencing the future studies and practical applications.

This document is a systematic review of the aspect of security and privacy of the IoT environment. It groups and names high-level threats to the IoT stack and proposes an analysis of the existing security and privacy-preserving mechanisms, their performance, and limitations. Moreover, it discusses new tendencies and gives future research directions to determine evolving security requirements of the IoT ecosystem. This review aims at achieving the following objectives:

- To categorize and analyse the security and privacy threats within the IoT settings
- Compare or study the available countermeasures
- To single out open problems and future directions of research.

II. BACKGROUND AND IOT ARCHITECTURE

Internet of Things (IoT) encompasses an ecosystem of devices and systems connected with each other to consume, share and analyze data to carry out smart actions. Knowledge on architecture of IoT is essential in helping to determine the vulnerability and security issues at every level of the system. Here, the typical IoT architecture description, its elements and actors, interaction and communication HP, and the connection between architecture and security are stated [3, 4, 5]. Figure 1 shows architecture of IOT.

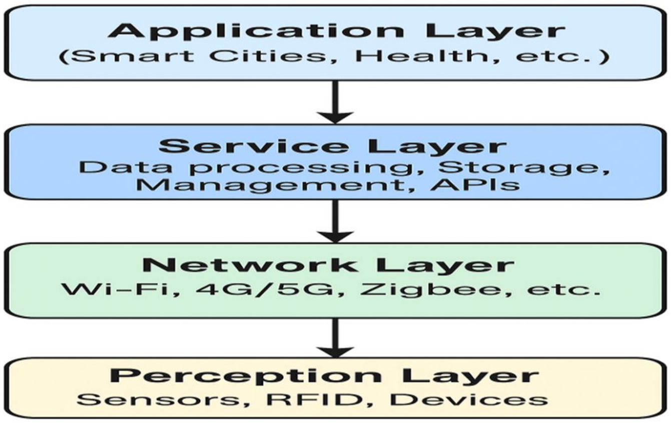

Application Layer
(Smart Cities, Health, etc.)
Service Layer
Data processing, Storage, Management, APIs
Network Layer
Wi-Fi, 4G/5G, Zigbee, etc.
Perception Layer
Sensors, RFID, Devices

Figure 1. IOT Architecture

A. Base level IoT (Perception, Network, Application Layers)

The IoT infrastructure is usually defined in three main layers:

- Sensing Layer: (The Physical layer of IoT architecture) This layer is also referred to as perception layer. It consists of all the gadgets and sensors which gather information of the environment. RFID tags, temperature sensors, motion sensors, GPS modules, and wearable devices are given as an example. This layer is the one that detects and aggregates data which is in turn transferred on to other layers.
- Network Layer: This layer is a boundary between perception layer and application layer. It sends the gathered information to diverse gadgets and frameworks with the assistance of correspondences like Wi-Fi, Bluetooth, ZigBee, 5G, or LoRaWAN. Network layer is composed of gateways, routers and clouds that help in the transfer of data, communication and identification of devices as well as routing of information.
- Application Layer- This is the highest layer and it provides application specific services to the end-users. It is data interpretation to make intelligent decisions and automation. These would be smartcity, industrial automation, healthcare monitoring and smart homes. This layer is closest to the users and is usually built with usage of cloud services, data analysis platforms, and mobile or web applications.

The layering implies the integration of certain security requirements and attack surfaces on each of the layers, so it is critical to look at the architecture as a whole when developing defense capabilities.

B. IoT System Components and Stakeholders

The IoT systems have a number of major components and stakeholders such as:

- Devices and Sensors: Specific hardware which gathers information and in some cases serves as an executing machine.
- Gateways and Hubs: They are the intermediaries which take care of connection of the devices and translation of the protocols.
- Cloud Platforms: Storage, analysis and IoT data management infrastructure.
- Applications: Programs that a user communicates with the system with the help of.
- Users: users/organizations providing/obtaining the IoT services.
- Service Providers: Companies which provide IoT platform, network or application hosting.
- Regulatory Bodies: If institutions controlling how security, privacy and data should be governed and strictly enforced they are referred to as the regulatory bodies.

Mutual collaboration and trust among these individuals is ensured data privacy and maintains the security of the data.

C. Communication and Information Exchange Protocol

IoT is based on the use of many communication protocols, and they depend on device power or range and power needs. Standard practices are:

Short-range Bluetooth, ZigBee, Z-Wave, NFC

- Medium: Wi-Fi, 6LoWPAN
- Long-range:Cellular (4G/5G), LoRaWAN, NB-IoT

Generally, the flow of the data is as follows:

1) Perception layer sensing and data collection
2) Gateway transmission or direct transmission to the cloud through the network layer
3) The cloud or edge-based infrastructure storage and analysis
4) Making decisions and interaction with the user via applications

This interception or disturbance in the flow of the information may lead to compromised integrity, confidentiality, or availability of a system. Encryption, authentication and secure communication protocol are therefore essential.

D. Architecture to Relevance to Security

The security issues of the IoT architecture at each layer are unique to one another:

- Perception Layer: The low computing power and physical accessibility makes it susceptible to physical tampering, injection of the fake data, and spoofing of the sensors.
- Network Layer: This layer is prone to eavesdropping, man-in-the-middle (MITM) attack as well as denial-of-service (DoS) when adequate encryption/authentication is lacking.
- Application Layer: It is vulnerable to threats like insecure APIs, bugs in software as well as unauthorized access to user information.

Knowledge of the architecture enables security designers to enforce layer-specific security at the sensor, secure routing protocols, use of intrusion detection systems at gateways and secure development techniques used in applications. Generally, layered defense (defense-in-depth) is required to secure the whole IoT system end-to-end.

III. SECURITY AND PRIVACY AND IOT

The heterogeneity and distributed characteristic of the IoT systems expose them to numerous forms of security and privacy challenges. These threats are capable of emerging on many levels, e.g., physical devices and communication frameworks, to cloud and human interfaces. This section categorizes and speaks on key challenges in five major categories [6][7][8].

A. Threats on the device level

- Physical Attacks

The IoT devices may be installed in unsecured or open places and can be easily subjected to physical attacks or destruction. Once physical access is obtained, the attackers will have direct access to the machine, where they can steal data or change settings or load malicious firmware. In high-stake systems like smart grid or automation of industries, the compromise of a single instrument is enough to break a whole system.

- Firmware Tampering

Those who conduct the attack can change or reprogram the firmware of IoT devices to create backdoors to them or to add malicious functionality. Even firmware is not well secured, so there are no checks to update or roll back firmware. Such threat invalidates the integrity of the device and has the potential of permitting continuous control by an adversary.

- Side-channel Attacks

The attacks leak information based on the physical use of a device, e.g., power consumption, electromagnetic emissions, timing information and use this to deduce sensitive information such as cryptographic keys. Such covert attacks are especially susceptible to many IoT devices because of their limited hardware protection.

B. *Threats at Network-level*

- Man in the middle Attacks (MITM)

In the case of the MITM attack, an adversary accesses and intercepts the communication between and across devices or even the device and cloud, and there is a risk of compromised or stolen confidential information. This can be especially hazardous in situations of nonencrypted or low-authenticated transferring of information.

- Denial of Service (DoS) and Distributed DoS (DDoS)

The purpose of such attacks is to overload an IoT device or IoT network with too much traffic and, as a result, become incapacitated. IoT botnets, such as the Mirai malware, have already provided evidence of the huge extent and harm such attacks can inflict on IoT networks and other internet services, in general.

- Eavesdropping and Packet Sniffing

Attackers can easily intercept unsecured or poorly encrypted communications information due to the relatively easy capture of data packets using simple spy tools. It may cause a leakage of information, credentials, control commands, or sensor data, which can be used as a basis to launch additional attacks.

C. *Threats of Data*

- Data Leakage

Mishandling the data may lead to unwarranted exposure, e.g., by using unencrypted data storage on local or cloud-based stored data. This becomes crucial especially in case of personal health information, monetary documents or location information.

D. *Threats to Data Data-related Threats*

- Data Leakage

Failure to treat the data appropriately may lead to unauthorized disclosure e.g storing data which is unencrypted in local memory or cloud servers. This is especially important when we are working with individual health and wellness, monetary or Geo-relevant information.

- Unauthorized Access

The absence of strong authentication and access control measures may give the opportunity to hackers to have access to IOT devices or platforms. When they get access, they are able to tamper data, shut down equipment or even use the equipment to further the attacks.

- Privacy Breaches

IoT gadgets usually record minute and constant data about a user, such as behavior, habits, and geographical position. In case such data is not appropriately secured, it may cause severe privacy breaching, profiling, and surveillance concerns.

E. Threats of Backend and Cloud

- *Insecure APIs*

As cloud platforms may be flexible and connected with various third-party services, APIs are often applied to communicate with a cloud platform and manage IoT devices remotely. Insecure API can be used by malicious parties to access systems, obtain contents or even tamper with system functionality.

- Data Storage vulnerabilities

The stored data can be misused or it can be used to portray a false truthful nature.Cloud-based storage systems which are not correctly encrypted, access-limited or isolated may be attacked by hackers to steal or corrupt sensitive information. Poor handling of access rights can result in exposing data to a third party.

- Cloud Misconfigurations

Configuration mistakes (publicly exposed storage buckets, unsecured administration console logins, default passwords) may make all IoT systems easily accessible to outside assailants. Being so common and widespread, these problems can be typical of IoT, which often depends on third party cloud services.

F. Human and Social Engineering Threats

- Phishing

Phishing emails or malicious login pages can also be used to factory IoT users or administrators of user and administrator accounts. Given that, hackers can take control of IoT devices and systems once hacked.

- Social Engineering

Attackers could also influence consumers to give them access or share information of personal value using tricks or fraud. Compared to technical vulnerabilities, the social engineering can exploit human behavior, thus it is more difficult to protect against its vulnerabilities.

- Insider Threats

Insiders, including the employees who are supposed to be using their legitimate access to IoT systems, may abuse their privileges in order to engage in malicious activities including data leakage, system disabling, or configuration changes. The insider attack is especially threatening as they frequently go through circumventing perimeter security. This variably finely grained threat environment speaks to a more readily born holistic and layered security strategy within IoT deployments. All the different threats affect the ecosystem in varying degrees and have different forms of counter strategies.

IV. AVAILABLE SECURITY PRACTICES AND PROGRAMS

1) Cryptographic Methods

- Light encryption
- Central approaches to management

2) Authentication and Access Control

- Two-factor authentication, multi-factor authentication.
- Role based access control (RBAC)
- Identity management solution

3) Intrusion Detection System (IDS)

- Anomaly based IDS
- Signature based IDS

4) Distributed Ledger and Blockchain

- Secure data sharing applications
- Building of trust

5) IoT Security using ML and AI

- Prediction of threats
- Automatic anomaly detection [9][10]

V. PRIVACY PRESERVING IOT.

Enhancing privacy in IoT systems is one of the key elements in the design, given the fact that these systems have a tendency to collect personal, behavioural and situational information. Various methods have been formulated to maintain privacy of the user by not affecting the functioning of the system [11][12].

A. Anonymization and Pseudonymization of data

Anonymization means the covering up or deletion of personal identifying information (PII) of datasets, rendering it hard to attribute the data to a unique person. Nevertheless, completely anonymous data can be less useful regarding analytics and occasionally such data can be resolved using sophisticated correlation.

Pseudonymization substitutes identifying field with artificial codes or pseudonyms. This method enables connecting the data between systems without giving out of actual identities and at times is reversible under authorised circumstances. It can find uses with regards to smart cities and medical purposes.

B. Differential Privacy

Differential privacy introduces statistical noise to the set of data or query responses, so as to ensure no inference can be made of an individual. A potential attacker can never make any deductions about the personal details of any person in the data set, even for those records that he or she might know. One application of differential privacy is that tech companies and governments employ it to estimate trade-offs between utility and privacy in their aggregated analytics using IoT devices.

C. Federated Learning

Federal learning enables the training of machine learning models to be computed on several devices or nodes, without exchanging raw data. The updates of the model are always sent to a central server so that the confidential information does not leave the local machine. It is optimal to be applied in IoT ecosystems where the mobile or edge device is present, including smart homes or wearables.

D. Secure Multi-Party Computation (SMPC)

SMPC allows several parties to permute a single function on their confidential data without exposing it to one another. The technique can be useful in cooperation-based IoT settings such as healthcare or industrial IoT since data sharing is essential but privacy is necessary.

VI. ANALYSIS OF EXISTING SOLUTIONS

Nevertheless, existing solutions to IoT security and privacy have their advantages and disadvantages despite all the progress that has been made [13][14].

A. Limitations and Strengths

Most of the available solutions offer strong protection against the known threats and aid in enforcing policies. They are however inconsistent and can not be optimized to handle dynamic attack vectors. Lightweight cryptography and federated learning are experiments with some success so far.

B. Overhead and Scalability of Performance

Such security mechanisms, in particular, cryptographic and blockchain ones may impose a computational and latency overhead. That is undesirable in real-time IoT systems such as autonomous cars, or industrial control networks. The volume of devices also becomes a problem since one will need to increase the scalability.

C. IoT Limitations in Resources

IoT-supported gadgets are usually low-power, low-storage, and low-compute. Strong encryption or AI-related defense of such devices is not possible without task offloading to cloud or an edge node.

D. Using and User Experience Problems

Security mechanisms should not make interactions with the user difficult. Insecure behaviors like disabling firewalls or reusing passwords, or poor adoption, may be the result of complex authentication or too many alerts. The IoT system design is usually lacking in usability testing.

VII. FUTURE RESEARCH AND FUTURE TRENDS

1) Zero Trust Architecture of IoT: Zero Trust philosophy holds to the idea of never trusting and always verifying. Using IoT as an example, that will have to be applied by implementing identity and access controls at the nodes. Such a model decreases the importance of the perimeter network security and is applicable to dynamic decentralized IoT [15][16].
2) Quantum Safe Cryptography: As there is a threat of quantum computing in the future, old encryption solutions such as the RSA and ECC might no longer be secure. Long-term data security the quantum-safe algorithms that are being developed include lattice-based algorithms or hash-based algorithms to provide long-term data security to the IoT deployments.
3) 6G and IoT Security Consequences: 6G will support ultra-low latency, high bandwidth, and support of mass devices. New standards, AI-native networking, and edges will bring new avenues of attack. It requires some research on how to design the security of the IoT architecture to 6G.
4) Privacy-by-Design Principles: Privacy-by-design is an architecture approach. It considers privacy as a part of the architecture instead of considering it as an afterthought. These are reduced data harvesting, localized processing, and transparency and user control on data use.
5) Security Edge or Fog Computing: Decentralization Processing performance and privacy are enhanced by edge and fog computing, processing it out beyond the server. Besides this however, they also provide new issues such as the need to secure local nodes and the handling of distributed trusts. New solutions include lightweight authentication, and encrypted containers.
6) Regulation and Policy Development (e.g. GDPR, NIST): Such regulations as the GDPR of EU or NIST guidelines are stimulating the adoption of secure-by-default. In the future, frameworks can be more targeted at IoT specific guidelines, which will require secure software updates, disclosure of vulnerabilities, and ethical use of data.

VIII. OPEN CHALLENGES

In the IoT security and privacy, important problems have not yet been addressed, in spite of the advances[17][18].

1) Interoperability and standardization: The issue of uniform standards, across various devices, operating systems and protocols, presents such challenges as compatibility, and a mismatch in security postures. Efforts shall be made to come up with international standards and certification.
2) Real-Time Threat Detection: On account of the dynamic characteristics of IoT systems, the conventional security models might not be able to track a risk or react to a risk in a timely manner. Detection of dynamically changing threats in real-time, based on AI, is only in active research.
3) Safe Update Methods: Most of IoT devices do not have over-the-air (OTA) updates or utilize insecure channels to live. This exposes them to a lifetime of exploitation. Easy, verifiable, and secure update systems should also be developed.
4) Security protocol energy-efficient: Security measures need to have a way of balancing security and energy consumption. Sensors or wearables powered by batteries need to have the best protocols so that they can last a long time without compromising security.
5) Trade-off of Usability over Security: It is difficult to create innovative but safe user interfaces. One of the main tasks of security solutions is to be seamlessly incorporated into users experiences so that they begin using them and do not cause their own vulnerabilities.

IX. CONCLUSION

The paper has provided an overview of the multi layered security and privacy issue which existed in an IoT environment, classified the major threats as well as analyzed some of the measures which are available. It emphasized the strengths and weaknesses of existing methods as well as the fast-growing opportunities such as blockchain, AI, and technology of keeping privacy. In the current world where IoT plays a very crucial part in every life, protecting such systems is not an option but a must. We need layers of passive and active defense that take account of the entire stack (sensors to cloud) in constructing a level of trust in IoT. In order to have a long-term security and scalability of IoT, it is necessary that future systems embed security and privacy in their system. Future developments of quantum-safe algorithms, decentralized trust models, and cross-national policy homogeneity will play important roles in defining secure and privacy-respecting IoTs.

REFERENCES

[1] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A., "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015. doi:10.1016/j.comnet.2014.11.008.

[2] Roman, R., Najera, P., & Lopez, J., "Securing the Internet of Things," Computer, vol. 44, no. 9, pp. 51–58, Sept. 2011.doi: 10.1109/MC.2011.291

[3] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[4] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[5] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, 2014, doi: 10.1109/JIOT.2014.2306328.

[6] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.

[7] R. Roman, J. Zhou and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013, doi: 10.1016/j.comnet.2012.12.018.

[8] R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010, doi: 10.1016/j.clsr.2009.11.008.

[9] A. R. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in Proc. 52nd ACM/EDAC/IEEE Design Automation Conf. (DAC), pp. 1–6, 2015, doi: 10.1145/2744769.2747942.

[10] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, Mar.-Apr. 2017, doi: 10.1109/MIC.2017.37.

[11] K. Zhang et al., "Security and Privacy in Smart City Applications: Challenges and Solutions," IEEE Communications Magazine, vol. 55, no. 1, pp. 122–129, Jan. 2017, doi: 10.1109/MCOM.2017.1600267CM.

[12] Badr, Y., Zhu, X. & Alraja, M.N., “Security and privacy in the Internet of Things: threats and challenges.”, SOCA 15, 257–271 (2021). https://doi.org/10.1007/s11761-021-00327-z.

[13] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

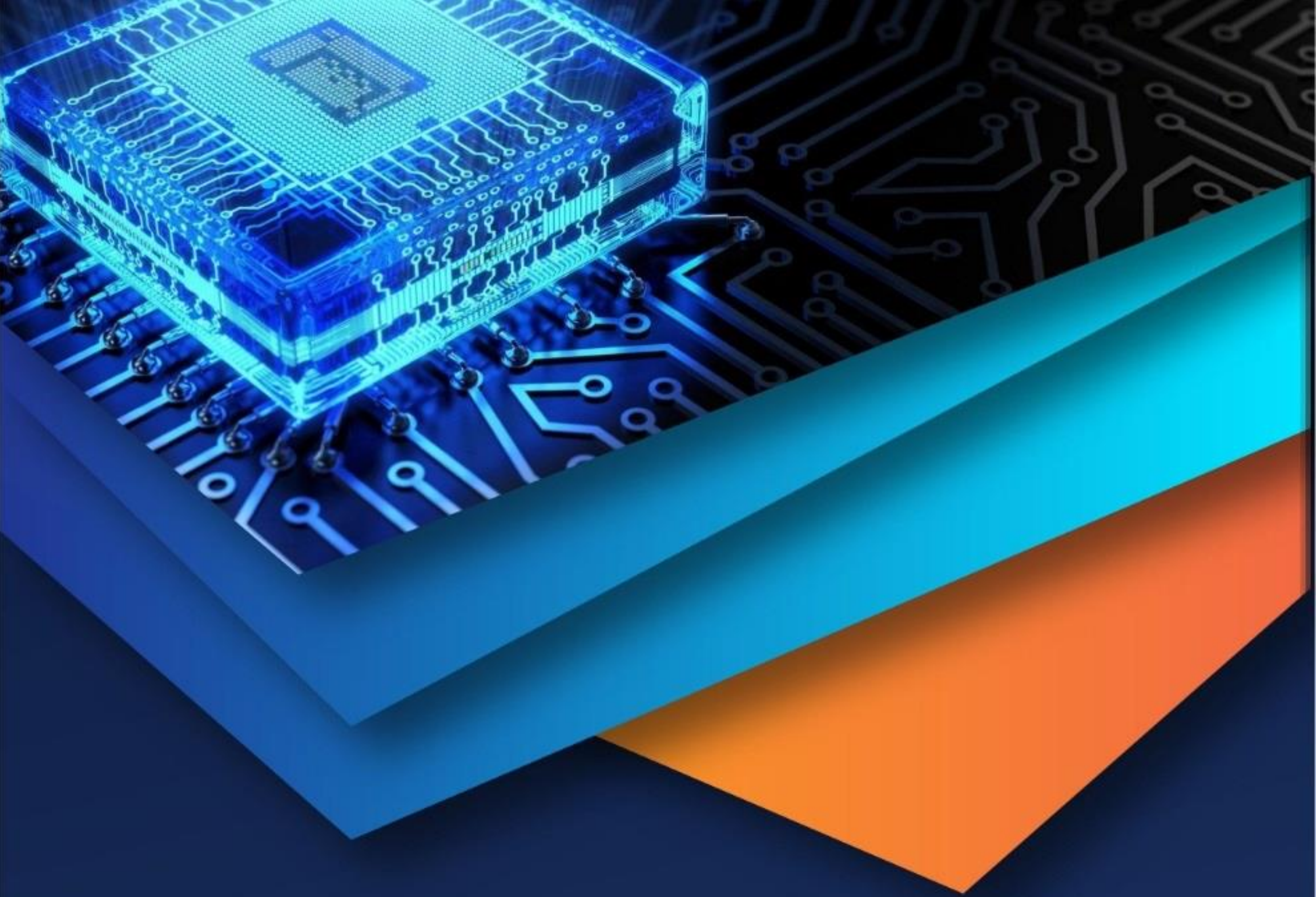
[14] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, New York, NY, USA, 2015, pp. 21-28, doi: 10.1109/SERVICES.2015.12.

[15] D. Miorandi, S. Sicari, F. De Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, Sept. 2012, doi: 10.1016/j.adhoc.2012.02.016.

[16] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431–440, 2015, doi: 10.1016/j.bushor.2015.03.008.

[17] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, vol. 54, pp. 1–31, 2014, doi: 10.1016/j.comcom.2014.09.008.

[18] F. A. Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017, doi: 10.1016/j.jnca.2017.04.002.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY