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.2025.73169

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 13 Issue VII July 2025- Available at www.ijraset.com

A Comprehensive Survey on Internet of Things (IoT), Architecture, Protocols, and Applications

Deepali Kawthekar[1], Pallavi Dakhore[2], Kalyani shevatekar[3], Bharat Shelke[4], Prajkta More[5]
[1]*Assistant Professor, Department of Computer science, DITMS College, Chh. Sambhajinagar*
[2]*Assistant Professor, Department of Computer Application, DITMS College, Chh. Sambhajinagar*
[3]*Assistant Professor, Department of Computer science, DITMS College, Chh. Sambhajinagar*
[4]*Associate Professor, Department of Computer science, SCS College, Omerga, Dharashiv*
[5]*Research Scholar, Department of Management Science, Dr.Babasaheb Ambedkar Marathwada University, Chh. Sambhajinagar*

Abstract: ***Internet of Things (IoT) is the phenomenon of digital environment that allows to transfer usual physical devices into computerized ones collecting, processing and sharing information via internet in small amount of human interaction. IoT, running on the next generation of embedded systems, wireless communications, and cloud computing, makes innovation possible in many fields, including healthcare, smart cities, agriculture, industrial automation, environmental surveillance. IoT systems, in which sensors, actuators, and data processing units are installed in real things, enable intelligent ecosystems to make the border between the real and the virtual worlds permeable. Generally designed in multi-lateral systems, with IoT being categorized in to perception, network and application layers, it guarantees the scalability and security of deploying systems. A multiplicity of protocols to support the varying degrees of interoperability and communication issues between heterogeneous devices have been invented to suit the various constraints on the power base, latency, bandwidth and mobility requirements. But with the evolvement of IoT, it has various challenges to contend with concerning standardization, security, data privacy, energy consumption and management of the devices. The paper gives an in-depth summary of the IoT ecosystem referring to its architecture, communication standards, and key areas of application, and is of great interest to the research, development, and practice researchers and developers who want to establish and develop efficient and productive IoT systems.***
Keywords: IoT, IoT Fundamentals, IoT Architecture, IoT Applications, IoT Protocols.

I. INTRODUCTION

IoT as a phenomenon is a revolution in the online space that allows ordinary physical devices to communicate, gather, and share data via the internet. IoT has become a technological cornerstone that edges innovation in various sectors namely healthcare, smart cities, agriculture, industrial automation, and environmental monitoring because of the swift development of related technologies like embedded systems, wireless communication, and cloud computing. It supplements the creation of smart surroundings through the combination of detectors, action elements, input/output structures, and information arranging capacities with physical items [1][2][3].

The essence of IoT is to allow a smooth transitional movement between the digital and physical world through a virtual network of appliances connected to each other, have ability to sense, process, and communicate with too little human input. IoT systems architecture normally has many tiers, such as perception, network, and application, with responsibilities and technologies of their own. These layers of architecture are key to the ability to scale and secure IoT implementation.

Due to interoperability needs and efficient communications between heterogeneous devices, numerous IoT communication protocols were developed. Such protocols address varying levels of networking protocols and support various power-related, bandwidth-related, latency-related, and mobility-related constraints. Selection of suitable protocols is vital in achieving performance, reliability and scalability in IoT implementations.

As IoT is multidisciplinary and its use is extensive, it is rapidly developing and presents a number of issues concerning standardisation, security, data privacy, energy efficiency and device management. In this paper, an overview of the IoT environment is provided, including its architecture, communication standard, significant areas of application. It is aimed to offer an integrated and analytical summary to researchers, developers, and practitioners concerned with designing and constructing effective systems of the IoT.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

II. IOT FUNDAMENTALS

A. Definition and Evolution of IoT

Internet of Things (IoT) is a term used to describe a huge network of connected physical objects which have sensors, software, and communication technology installed in them to allow the collection, transferring, and reacting to data with the minimum of human effort needed. The aim of the IoT is to create a seamless transition between the physical and digital environment so that the objects and systems can communicate in a smart way[4][5].

IoT can be dated as early as the 1980s with hooked up vending machines and significantly developed in the late 90s when Kevin Ashton introduced the term Internet of Things in his employment at Procter&Gamble. Since this era, IoT has expanded at a very high pace because of the advancement of wireless communications, sensor technologies, cloud computing, and data analytics. In recent years, IoT preconditioned digital transformation in many industries, and its innovations include smart homes, connected healthcare, autonomous vehicles, etc.

B. Key Characteristics and Features

IoT systems also present a number of defining features, which distinguish them among conventional computing systems[6]:

- Interconnectivity: Systems and devices are joined together on either wireless or wired communication.
- Autonomous Operation: Equipment can work with little or lack of human contact.
- Scalability: IoT systems may be scaled by increasing the number of devices connected to the network to the billions.
- Context-Awareness: It is the ability to sense and react to the world.
- Intelligence: The ability to make clever decisions due to the integration with AI/ML.
- Heterogeneity: There is a lot of differences in terms of hardware, software and communication ability of devices.
- Low Energy Use: As low power consumption is desirable and particularly in battery powered equipment.

C. Components of IoT Systems

An IoT design normally entails the following main elements[7]:

1) The Sensors and Actuators

The detection and measurement of some physical parameters (temperature, humidity, motion, pressure, and light) are the responsibility of the sensors. Actuators on their part takes physical actions on processed data i.e. opening a valve, switching on a light or changing the speed of a motor. Such elements constitute the perception layer of IoT and constitute the bridge between the real and the virtual worlds.

The system of IoT usually includes the following main elements[7]:

2) Modules in Sub-system connectivity

The communication between the IoT devices and other systems or the cloud is possible due to connectivity modules. Such modules profile multiple communication protocols and technologies, e.g. Wi-Fi, Bluetooth, ZigBee, LoRa, NB-IoT, and cellular networks (e.g. 4G/5G). The connectivity option is subject to selecting factors such as range, data rate, power consumption and application need.

3) Data Processing Units (DPUs)

The processing of data is usually conducted by data processing units, such as microcontroller, edge devices, or cloud servers and deals with analysis, filtering, and interpretation of sensor data. These units are either embedded into a device (edge computing) or run at distance through a cloud infrastructure depending on the latency, security and computational needs.

D. IoT development difficulties

Although it has potential, development of IoT is confronted by a number of technical and non-technical challenges [8]:

- Security and Privacy: IoT systems are susceptible to malicious break-ins and hacking due to their distributed design and the fact that IoT devices have little computational power
- Interoperability: There are no standardized guidelines and protocols, which prevent full interoperability between heterogeneous devices and operating platforms.
- Scalability: Supporting and servicing an increasing number of connected devices is a complicated process that needs an elaborate infrastructure.

©IJRASET: All Rights are Reserved

- Energy limits: Most IoT devices are limited based on energy sources, thus they require low energy designs.
- Data Management: The management of these big data flow captured in real time is high capacity in regard to storage, efficient data transmission, and analytics.
- Deployment Cost and Complexity: The network can be expensive to set (and maintain), and the initial cost of of adoption may be prohibitive.

III. IOT ARCHITECTURE

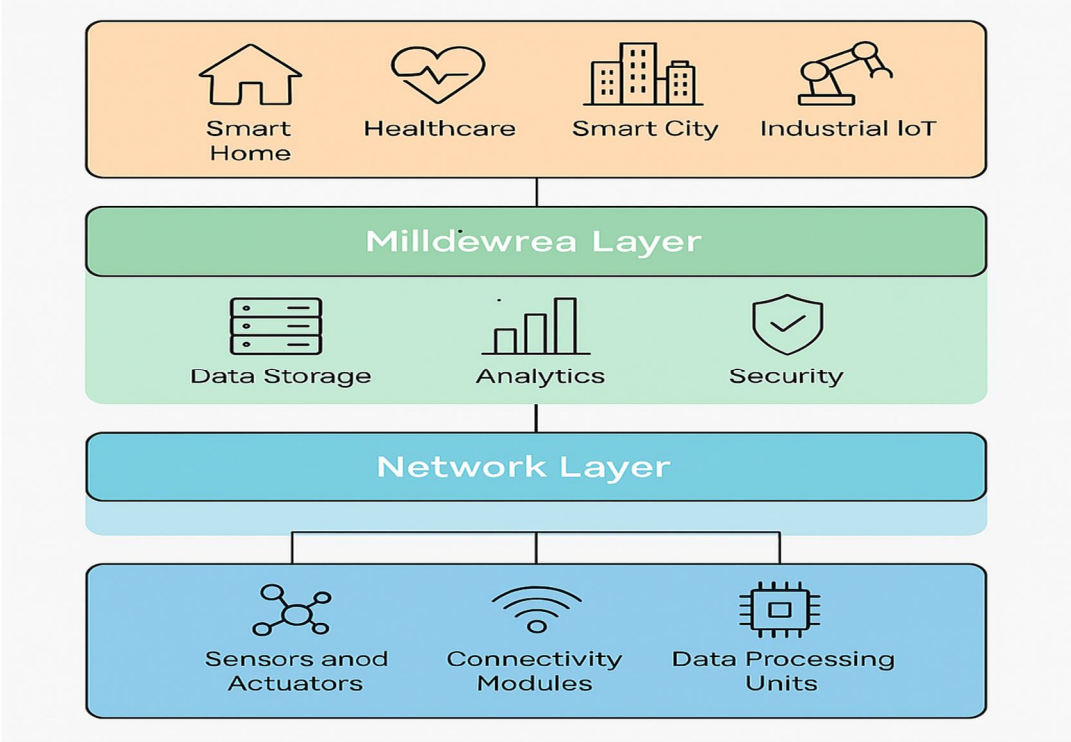


Figure 1: show IoT Architecture

Internet of Things (IoT) [9]-based architecture shown in Figure 1 not only offers a systematic method to identify the IoT-based data generation, transmission, processing, and usage within an IoT ecosystem, it also provides a standard guide on how to implement the process. The creation of IoT solutions requires the clear architecture that would support the scalable and interoperable solutions and were effective. In spite of a number of the architectural models in existence, layered architecture model is commonly used because of its modular layout and its well-defined division of concerns. There are four layers in the typical IoT architecture, including the Perception Layer, Network Layer, Middleware Layer, and the Application Layer.

A. Layered Architecture of IoT

1) Perception Layer

Internet of Things (IoT) [9]-based architecture not only offers a systematic method to identify the IoT-based data generation, transmission,processing, and usage within an IoT ecosystem, it also provides a standard guide on how to implement the process. The creation of IoT solutions requires the clear architecture that would support the scalable and interoperable solutions and were effective.

In spite of a number of the architectural models in existence, layered architecture model is commonly used because of its modular layout and its well-defined division of concerns. There are four layers in the typical IoT architecture, including the Perception Layer, Network Layer, Middleware Layer, and the Application Layer.

2) Network Layer

This layer sends the data which is received in the perception Layer to the middleware or to the cloud Platform. It provides safe, trustworthy and effective system of transferring data among the devices and the bearers of processing information. It entails several technologies and communication protocols.

Key Functions:

- Data directing and transferring
- Handling connection with devices
- Encourage technologies of communication such as Wi-Fi, Bluetooth, 5G, ZigBee, LoRa, etc.

3) Middleware Layer

The middleware layer plays the role of mediating between the network and application layer. It stores, processes and makes decisions on data. It offers services such as device management, data filtering, security and orchestration of the services.

Key Functions:

- Management and data analysis
- Registration and surveillance of device
- Service and API management

4) Application Layer

The Application Layer is the uppermost one which provides smart services to the end users depending upon the processed data. It facilitates numerous applications that are specific to various fields including medical, farming, intelligent city, and factory automation.

Key Functions:

- Service (domain specific) delivery
- Management of user interface
- Insights and alert visualization

B. Edge and Fog Computing in IoT

Conventional IoT systems involve cloud computing and it may induce latencies and bandwidth concerns. In order to deal with this, Fog Computing and Edge Computing have come into existence.

Edge Computing is a type of computing that provides data processing close to its origin (i.e. at the device level). It is perfect in the real-time decision-making. Fog Computing as proposed by Cisco, builds on the capabilities of cloud computing by moving the processing nodes (referred to as fog nodes) even closer to the sources of data thus providing a distributed computing environment.

The given approaches will make them more responsive, minimize data transmission cost, and improve privacy and reliability of time-sensitive IoT applications.

C. Cloud-based IoT Architectures

Cloud computing is at the center of IoT, as it provides scalable storage capabilities and potent computing and real-time analytical skills. In a cloud IoT:

Sensors transmit their data to the cloud servers where information is processed and stored permanently.

Cloud platforms integrate services consisting of device management, dashboards, alerting, and machine learning models.

Some of the platforms to consider cloud-based IoT include AWS IoT Core, Microsoft Azure IoT Hub and Google Cloud IoT.

Mass IoT can be served with cloud-based structures as they can sustain elasticity, central administration, and ubiquity.

D. Interoperability and Integration Challenges

Architectural problems notwithstanding, the aspect of interoperability and integration proves to be another significant roadblock on the development of IoT:

- Various Protocols: IoT devices employ different communication protocols (e.g., MQTT, CoAP, HTTP), which causes incompatibility.
- The Heterogeneous Devices of devices: There is a difference in devices in terms of hardware, OS, data format, and capabilities.
- Existence of No Standard: There are no common standards that can facilitate a smooth integration of devices.

- Data Silos: Data may become separated and isolated due to vendor specific solutions.
- Security and Privacy: Issues of security and privacy are increased due to integrating devices across domains and complexity of end-to-end security potentially is introduced.

The solutions to these issues would be found in using open standards, middleware frameworks, and universal APIs, which guarantee the interoperability and the scaleability of the IoT systems.

IV. IOT COMMUNICATION PROTOCOLS

Summary of the Communication Requirements

IoT communication policies facilitate easy transfer of information to and among various devices. Communication requirements are[10]:

- Minimal consumption of power
- Low latency
- Reliability
- Scalability
- Security
- Multi-device / multi-platform interoperability

The IoT protocols have been designed in forms of the OSI model and served on different layers to fulfill different functions.
Various-Layer Protocols:

1) Layer of perception protocols

The protocols will enable communicating with a device at lower levels, and wireless communications over a short distance.

- RFID (Radio Frequency Identification): This is applied on labeling and monitoring items.
- NFC (Near Field Communication): Supports short range communication of devices.
- ZigBee: An energy-efficient, low and slow wireless specification well suited to home automation and light industrial control scenarios.
- Bluetooth: Short distance radio communication; Bluetooth Low Energy (BLE) It is specialized in IoT.

2) Network Layer Protocols

These are the protocols that deal with diversion and directing of data among the IoT gadgets and the internet.

- IPv6: Allows extremely high amount of distinct IP addresses of devices.
- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks): Adaptation protocol which can enable IPv6 throughout low power networks such as IEEE 802.15.4

RPL (Routing Protocol for Low-power and Lossy Networks): A protocol created to route efficiently in an Internet of Things network; distance-vector protocols.

3) The Transport Layer Protocols

These are in charge of end to end communication and data is delivered reliably or within time as required.

- TCP (Transmission Control Protocol): It guarantees reliability, sequence and error-controlled transmission of data.
- UDP (User Datagram Protocol): Provides expedited transmission that is not guaranteed and can be useful with time sensitive data.

4) The application layer protocols

This layer code provisions data format, transmission, and interoperability of IoT applications.

- MQTT (Message Queuing Telemetry Transport): It is lightweight publish-subscribe protocol which is designed to suit constrained devices and low-bandwidth networks.
- CoAP (Constrained Application Protocol): a web transfer protocol optimized and used to deal with low power electronic hardware.
- AMQP (Advanced Message Queuing Protocol): This offers security, routing message orientation, and queuing.

Comparison and selection criteria of protocols:

The protocol implementation relies on application specifications. The main criteria of selection are:

- Power consumption
- Data rate and payload size
- Latency and real-time performance
- Security features
- Support to network topology
- Ability to work with the other systems

V. IOT APPLICATIONS

Almost every industry has been impacted by the Internet of Things (IoT), which has changed how systems communicate, automate tasks, and make judgements. Key IoT application areas are listed below [11][12]:

A. Building and Home Automation

In smart houses, IoT devices are used to automate, as well as remotely control their light fixtures, heating, air conditioning systems, appliances, security solutions, and energy consumption. The use of voice assistants such as Alexa or Google home is aimed at increasing convenience of use. Smart buildings in the commercial environment are based on sensors to minimize energy consumption, space and occupancy comfort.

B. Wearables Healthcare

IoT in the healthcare industry will provide possibilities of patients being monitored remotely, chronic conditions, intelligent diagnostics, and emergency call systems. Fitness bands and highly portable devices (such as ECG monitors) generate real-time health data, which is processed, and evaluated to identify anomalies and aid in medical choices.

C. Towns and Smart Cities

The redesigned infrastructural and services in smart cities are performed via IoT. Its application will be used in smart traffic management, smart lighting on the streets, smart waste management, air quality monitoring, and emergency systems. These remedies add value to life and save consumption.

D. IIoT (Industrial Internet of Things) and Industry 4.0

IIoT links the equipment, equipment, and control overall in the manufacturing setting. It allows the ability to perform predictive maintenance, monitor in real-time, and automate, which helps in achieving Industry 4.0 objectives of becoming more productive, having minimal downtime, and more intelligent supply chains.

E. Monitoring with reference to Agriculture and Environment

The IoT applications in the agricultural sector are used to make precision agriculture by tracking soil moisture, temperature, and crop condition. Automated irrigation, drones and sensors can be used to enhance yield without wasting resources. Likewise, environmental monitoring systems monitor pollution, water level, and weather condition.

F. Logistics and Transportations

IoT increases tractability of vehicles, fleet control and logistics. Intelligent sensors are used to observe the state of vehicles, the situation on the road, and the security of cargo. The passenger information, the route optimization and the accident prevention technologies increase the benefits of a public transport system.

G. Field Trial and Operational Deployments

1) John Deere: Employs IoT in the precision agriculture area by using connected sensors and connected tractors.

2) GE Predix Platform: It enables the management of industrial asset actions in manufacturing facilities.

VI. PRIVACY AND SECURITY OF IOT

Security IoT security is a burning issue since there are many connected devices, and the data is sensitive[13].

1) Common Vulnerabilities and Threats

- Secure interfaces and APIs
- Poor passwords or standard ones
- No encryption
- Man in the middle attacks and device spoofing
- Damage on hardware or firmware modification

2) Layer Requirements of Security

- Perception Layer: Secure boot, physical protection
- Network Layer: safe communication protocols (e.g. TLS/DTLS)
- Middle ware Layer: Access control, anomalous detection
- Application Layer: secure APIs, access control of the user

3) Mechanisms that Preserve Privacy

Some methods of privacy protection include:

- Data anonymization
- Safe data compilation
- Data sharing on the basis of consent
- Analytical differential privacy

4) Computationally Light Cryptography and Authentication

IoT devices have limited resources and need effective cryptography algorithms. Stream ciphers, like PRESENT and HIGHT, and other lower-end methods of authentication including ECC and hash-based signatures are developed to make sure that security is achieved without strain on the device capabilities being reached.

5) Where to Go on IoT Security?

- Threat detection based on AI[14].
- Decentralized trust based on block chain
- Uniformity of IoT safety systems

VII. RESEARCH TOPICS AND DIRECTIONS CHALLENGED

Even though it has been growing, IoT still experiences a lot of challenges [15]:

1) Interoperability and Standardization: A global standards dearth is one of the barriers to integration within various IoT platforms and device producers. There is a research need within the scope of developing universal standards of protocol, data format, and interoperability framework.

2) Energy-effectiveness and Power inch Space: Several IoT devices use power supply that is restricted. Research of efficient energy harvesting, sleep modes and low power communication protocols is necessary.

3) Managing and Analysing Big Data: The data generated by IoT is extremely large in amounts, and as such, it requires scalable storage, processing in real-time, and filtering intelligence. The combination of big data platforms such as Hadoop and Spark with IoT is the subject of research.

4) IoT Networks scalability: As the connected devices proliferate, it becomes more complicated to maintain network performance, address schemes (such as adoption of IPv6), and reducing latency.

5) AI and ML in IoT to Intelligent Decision-making: IoT can use edge and cloud systems by embedding AI/ML models, which will improve decision-making. Work is being done on federated learning and model optimization to edge devices and real-time inference.

6) Concerns regarding Regulation and Ethics: Some of the concerns identified with IoT are spying, private data, user consent and ethics. It will require policies and laws to change in order to become responsible and transparent in their deployment.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VIII. CONCLUSION

The Internet of Things is changing the way devices are connected, processed and acted upon based on real-life scenarios. This survey has given a broad picture of the architecture of IoT, important communication protocols, applications and security models.

We studied gradation of IoT systems, described the meaning of edge/fog/cloud computing, and named the examples of implementation in particular domains starting with smart homes and going to industrial automation. Such current issues as interoperability, energy efficiency, data management, and security concerns were discussed as well.

To the academic community, this survey will give lessons about center concepts, future lines of research. It presents opportunities of innovation and optimization of industries.

In the future in which IoT is progressing, interdisciplinary collaboration, the ethics of technological development, and self-sustaining technological progress will be prerequisites in achieving what it is capable of transforming completely.

REFERANCES

[1] Kailas, V., Nivrutti, S., & Atul, S. (2024). A Detailed Study of An Internet of Things (IoT): Review, Recent Research Directions and Complete Journey Towards Sustainable and Smart Future. International Journal of Advanced Research in Science, Communication and Technology. https://doi.org/10.48175/ijarsct-19373.

[2] Maheshwary, P. (2024). Review of: “Internet of Things in Smart Grid: A Comprehensive Review of Opportunities, Trends, and Challenges.” https://doi.org/10.32388/puzzjl

[3] Bhattacharya, S., Kumar, R., & Singh, S. (2020). Capturing the salient aspects of IoT research: A Social Network Analysis. Scientometrics, 125(1), 361–384. https://doi.org/10.1007/S11192-020-03620-4

[4] Arshi, O., & Chaudhary, A. (2024). Fundamental Concepts of IoT. 42–69. https://doi.org/10.1201/9781032656694-2

[5] Jha, M. K., Singh, M., & Sahoo, A. (2021). Fundamental Principles of IoT (pp. 1–25). IGI Global. https://doi.org/10.4018/978-1-7998-4775-5.CH001

[6] Tamrakar, A. K., Shukla, A., Kalifullah, A. H., Reegu, F., & Shukla, K. (2022). extended review on internet of things (IoT) and its characterisation. International Journal of Health Sciences (IJHS), 8490–8500. https://doi.org/10.53730/ijhs.v6ns2.717

[7] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). *Internet of Things (IoT): A vision, architectural elements, and future directions*. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

[8] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). *Internet of Things: A survey on enabling technologies, protocols, and applications*. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[9] A. A. Mohammed, M. S. Hossain, M. A. Rahman, M. A. Alzain, and M. A. Alshamrani, "Internet of Things: A comprehensive overview, architectures, applications, simulation tools, challenges and future directions," *Discover Internet of Things*, vol. 4, no. 1, pp. 1–33, 2024. [Online]. Available: https://doi.org/10.1007/s43926-024-00084-3

[10] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A Survey of Communication Protocols for Internet-of-Things and Related Challenges of Fog and Cloud Computing Integration," *Int. J. Distrib. Sens. Netw.*, vol. 14, no. 7, pp. 1–26, Jul. 2018,

[11] P. Shao et al., “A review of IoT applications in healthcare,” *Neurocomputing*, vol. 565, Jan. 2024, Art. no. 127017.

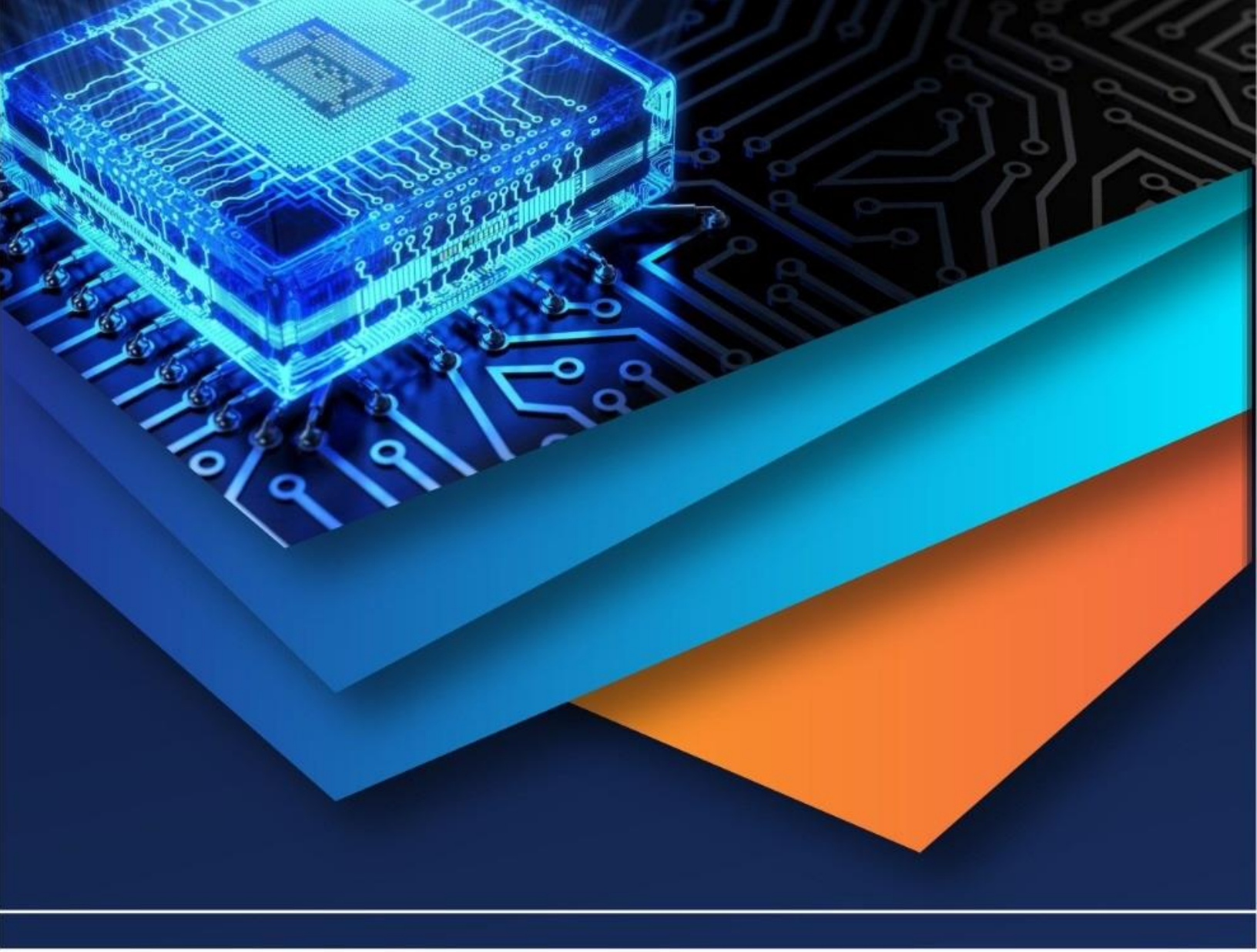
[12] M. R. Karim, A. Al-Ameen, K. Sultana, M. K. D. Hossain, and M. R. Hasan, “A comprehensive survey on IoT and AI based applications in different pre-harvest, during-harvest and post-harvest activities of smart agriculture,” *Comput. Electron. Agric.*, vol. 216, Jan. 2024,

[13] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A survey of IoT security based on a layered architecture of sensing and data analysis,” *Sensors*, vol. 20, no. 13, Art. no. 3625, Jul. 2020.

[14] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, “A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review,” *Sensors*, vol. 23, no. 8, Art. no. 4117, 2023.

[15] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, “Reliable Internet of Things: Challenges and Future Trends,” *Electronics*, vol. 10, no. 19, art. 2377, Sep. 2021.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)