Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

# INTERNET OF THINGS: APPLICATIONS, SECURITY, PRIVACY AND FUTURE PROSPECTS

**Meerub Akhtar[*1], Khadija Ishaq[2], Laiba Jabeen[3], Ateeb Ur Rehman[4]**

[*1,2,3,4]*National university of Modern Language, Department of software Engineering, NUML FSD*

[*1]meerubakhtar@4gamil.com, [2]bakhtawarishaq93@gmail.com, [3]jabeenlaiba34@gmail.com, [4]ateebmirza323@gmail.com

DOI:https://doi.org/10.5281/zenodo.20701373

**Keywords**
*Internet of Things, Security, Privacy, Authentication, Applications, Access Control*

**Article History**
*Received: 18 April 2026*
*Accepted: 30 May 2026*
*Published: 15 June 2026*


**Corresponding Author: ***
**Meerub Akhtar**

**Abstract**
*The Internet of Things (IoT) is used in homes and hospitals as well as in outdoor spaces to monitor and report environmental. More useful functions. By perceiving, communicating, and acting smart in different situations, the Internet of Things (IoT) has become a major technological model of the digital age. IoT transforms traditional systems into intelligent infrastructures that enhance automation, efficiency, and decision-making across several domains, such as manufacturing, transportation, healthcare, and agriculture, by integrating sensors, embedded systems, and communication networks. The great security and privacy concerns occasioned by the enormous quantity and variety of IoT devices cannot be overstated. IoT systems are vulnerable to numerous cyber-attacks and privacy breaches based on resource depletion, weak authentication, and insecure communication protocols, and inadequate data security practices. Internet of Things' architecture, its primary applications, and the key security and privacy issues jeopardizing its reliability are comprehensively discussed in this research. It examines existing security practices such as access control models, authentication schemes, and encryption techniques while highlighting the growing role of blockchain, AI, and machine learning in the development of advanced IoT defense systems. The paper also deals with the legal and ethical implications of IoT data management and examines prospective directions for future work to build IoT frameworks that are scalable, lightweight, and privacy-preserving. The research concludes that it is crucial for building a secure and trustworthy IoT environment to have a holistic approach integrating user-centric privacy models, technological innovation, and compliance with the law.*

## 1. INTRODUCTION

One of the most innovative ideas shaping today's digital era is the Internet of Things (IoT). It simplifies communication between the real and virtual worlds by combining smart devices, embedded systems, sensors, and intelligent software. This technology changes traditional processes into smart, automated environments by allowing things to collect, share, and analyze data with little human involvement. The basic idea behind the Internet of Things is to create a future where every device, from industrial machines to household appliances, can be controlled, monitored, and connected over the Internet. Advancements in several areas, including wireless sensor networks, artificial intelligence, cloud

computing, and nanotechnology, form the basis of the Internet of Things.

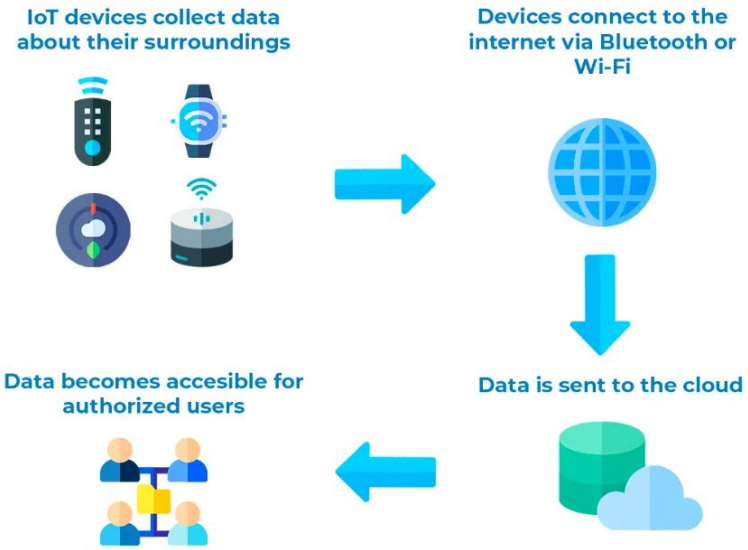


**Figure 1 1: IOT Initial Working**

IoT not only improves productivity across various industries, but it also creates large amounts of data that aid in forecasting and decision-making. Globally, the rapid growth of IoT has brought important social and economic effects. With the idea of Industry 4.0, governments and businesses are investing heavily in connected healthcare, smart manufacturing, and smart city projects. IoT devices are becoming faster, more reliable, and more energy-efficient due to 5G networks and edge computing technology. However, this same connectivity that enhances IoT also exposes it to serious security and privacy threats. Unauthorized access, data leaks, identity theft, and network breaches are likely when billions of devices communicate at once.


**Figure 1 2: Home Security**

Creating strong encryption and authentication systems is tough since most IoT devices have limited energy, storage, and processing power. Additionally, many devices use outdated firmware or lack standard security measures, making them vulnerable to data misuse and cyberattacks. As we move closer to a fully connected world, IoT will also expand into new areas like smart infrastructure, personalized medicine, and smart government. However, issues of cybersecurity, trust, privacy, and authentication must be addressed to realize its full potential. Future success in IoT will depend on how effectively it can protect user security and privacy in an increasingly digital and data-driven society, alongside technological advancements.


**Figure: Policies of IOT**

This figure highlights the key policies governing the implementation and use of IoT technologies. These policies ensure data privacy, security, and ethical usage of connected devices across various sectors. They also provide guidelines for interoperability, standardization, and responsible data sharing to enable safe and efficient IoT adoption.

### 1.1 Problem Statement

The Internet of Things (IoT) is rapidly expanding across various domains such as healthcare, smart homes, agriculture, and industrial systems. Despite its significant benefits in automation and real-time data processing, IoT systems face several critical challenges that hinder their secure and efficient deployment.

- **Security Risks in IoT Systems**: IoT environments are highly vulnerable to cyber-attacks due to weak authentication mechanisms, insecure communication channels, and insufficient encryption techniques.
- Attackers can exploit these weaknesses to launch threats such as unauthorized access, data manipulation, denial-of-service (DoS) attacks, and device hijacking.
- Since IoT devices are often deployed in large-scale and distributed networks, securing every node becomes a complex and difficult task.


**Figure 1 3: Vulnerabilities and Attack vectors**

**Privacy Leakage Issues:** IoT devices continuously collect and transmit sensitive user data such as personal behavior, location, health records, and environmental information. This creates serious privacy concerns, as unauthorized parties may access or misuse this data. Lack of proper data control, transparency, and user consent mechanisms increases the risk of privacy violations and surveillance issues.

**Device Limitations:**

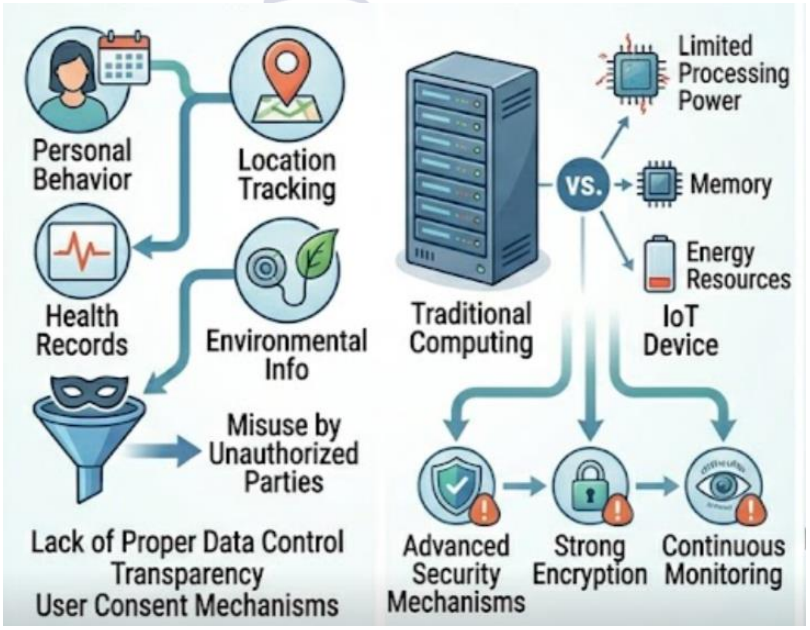


**Figure 1 4: limitation of Work**

Most IoT devices are designed with limited processing power, memory, and energy resources. Due to these constraints, it becomes difficult to implement advanced security mechanisms such as

strong encryption, complex authentication protocols, and continuous monitoring systems. These limitations make IoT devices more vulnerable to attacks compared to traditional computing systems. **Lack of Standardization:** IoT systems consist of heterogeneous devices, platforms, and communication protocols developed by different manufacturers. The absence of global standards leads to interoperability issues, inconsistent security implementations, and integration challenges.

### 1.2 Background

With the ability to seamlessly connect physical items, sensors, devices, and networks over the internet, the Internet of Things (IoT) is a paradigm shift in contemporary computer and communication systems. By enabling real-time data collection, sharing, and analysis amongst devices, its main goal is to close the gap between the digital and physical worlds. IoT systems combine network, hardware, and software elements to build intelligent spaces that can perceive, process, and respond without much assistance from humans. In order to improve efficiency, automation, and decision-making, this idea expands the traditional Internet by integrating billions of networked devices, including wearables, sensors, actuators, cars, and home appliances.

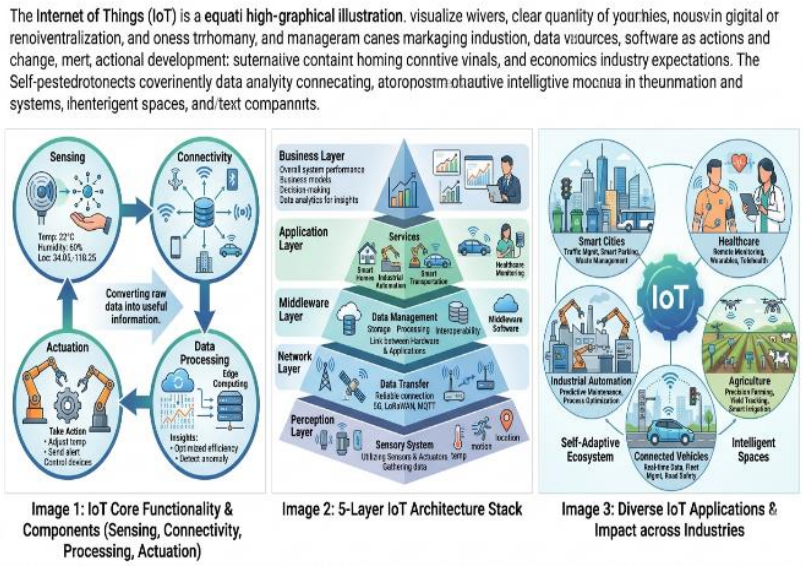


Image 1: IoT Core Functionality & Components (Sensing, Connectivity, Processing, Actuation)

Image 2: 5-Layer IoT Architecture Stack

Image 3: Diverse IoT Applications & Impact across Industries

**Figure 1 5:Core Functionality**

Sensing, connectivity, data processing, and actuation are the four primary components that make up the core operation of the Internet of Things. Sensing devices gather environmental data, including location, motion, temperature, and humidity.

- Following that, this data is sent over communication networks using a variety of protocols, including Bluetooth, Zigbee, Wi-Fi, and cellular connections.
- The data is processed and analyzed to extract valuable insights once it reaches cloud platforms or edge computing devices.

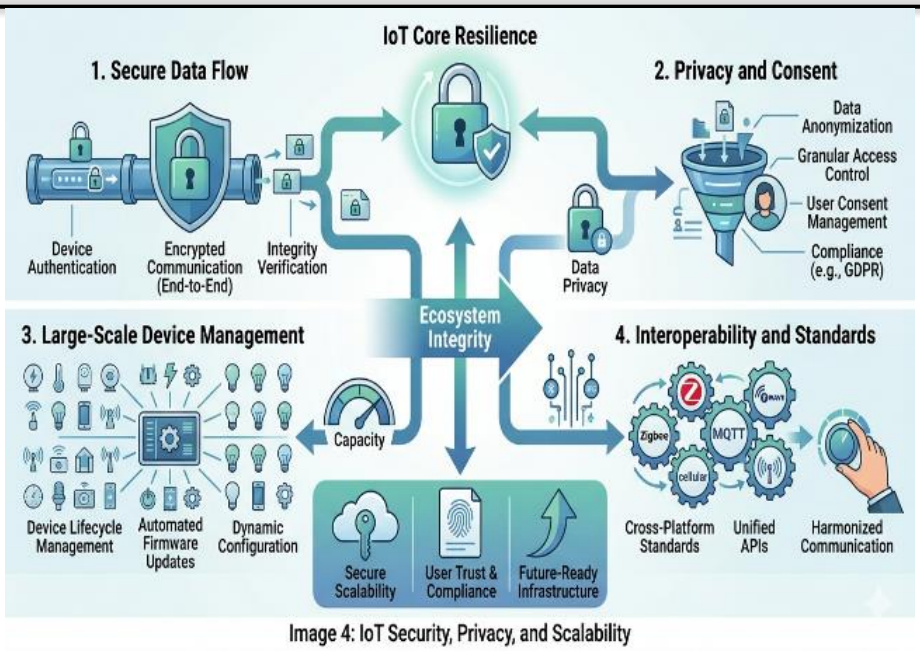


**Figure 1 6: Iot security, privacy, and scalability**

The middleware layer controls data storage, processing, and interoperability among heterogeneous devices, acting as a link between hardware and applications. Certain services, such intelligent transportation, industrial automation, smart homes, and healthcare monitoring, are provided via the application layer. Lastly, the management of overall system performance, business models, and decision-making procedures based on IoT data analytics are the main objectives of the Business Layer.

**Table1: Layers of iot**

| Layer Name | Sensing & Data Collection | Connectivity & Transmission | Data Processing & Middleware | Business Logic & Strategy |
|---|---|---|---|---|
| Perception (Sensing) Layer | ✓ | ✗ | ✗ | ✗ |
| Network (Connectivity) Layer | ✗ | ✓ | ✗ | ✗ |
| Middleware (Processing) Layer | ✗ | ✗ | ✓ | ✗ |
| Application Layer | ✗ | ✗ | ✓ | ✗ |
| Business Layer | ✗ | ✗ | ✗ | ✓ |

IoT essentially functions as a self-adaptive ecosystem by combining data sensing, communication networks, cloud or edge computing, and intelligent analytics. Its tiered architecture guarantees that information is safely recorded, sent, and used to provide useful insights. Across addition to increasing scalability and interoperability, this multi-layered strategy increases the usefulness and dependability of IoT.

### 1.2 Objectives

- To study the fundamental concept of the Internet of Things (IoT) and understand how

interconnected devices communicate, collect, and exchange data in real-world environments.

- To analyze different IoT architectures (such as three-layer and five-layer architectures) in order to understand their structure, functionality, and role in data processing and communication.
- To explore major applications of IoT in various domains including healthcare, agriculture, smart homes, industrial automation, and smart cities.
- To identify security and privacy challenges in IoT systems, such as authentication issues, data breaches, unauthorized access, and resource constraints.

### 1.3 Literature Review

Over the last ten years, research on the Internet of Things (IoT) has grown significantly, resulting in a rich yet dispersed body of literature covering middleware, applications, architectures, security, privacy, and supporting technologies.

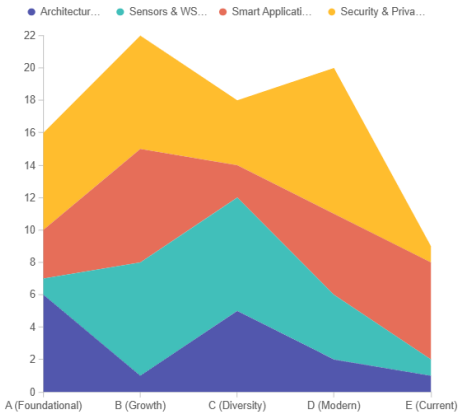


**Figure 1 7: Comparison of architecture**

The conceptual layers of IoT and the cataloged technologies (sensors, RFID, WSNs, communication stacks, and cloud/edge computing) that provide ubiquitous sensing and connectivity were developed by early surveys and foundational research. In order to provide real-world improvements in efficiency, safety, and decision support, later research has concentrated on domain-specific applications in the fields of healthcare, smart cities, agriculture, industrial automation, transportation, and logistics.

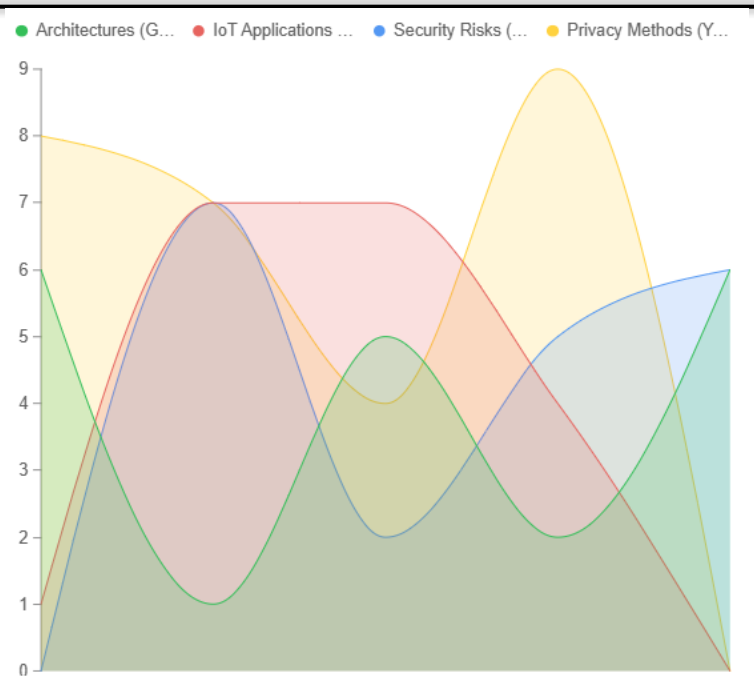


**Figure 1 8: Line Graph of architecture**

Numerous mitigation strategies have been assessed by researchers, including role-based or attribute-based access control models, mutual authentication and PKI-based schemes, secure communication stacks (TLS/DTLS, MQTTS, CoAP+DTLS), secure boot and code-signing to guarantee firmware integrity, and lightweight cryptography for devices with limited resources. IoT privacy research has evolved alongside security research, although it frequently focuses on distinct issues, such as location privacy, consent/ownership models, data-mining dangers, and user profiling via continuous sensing.

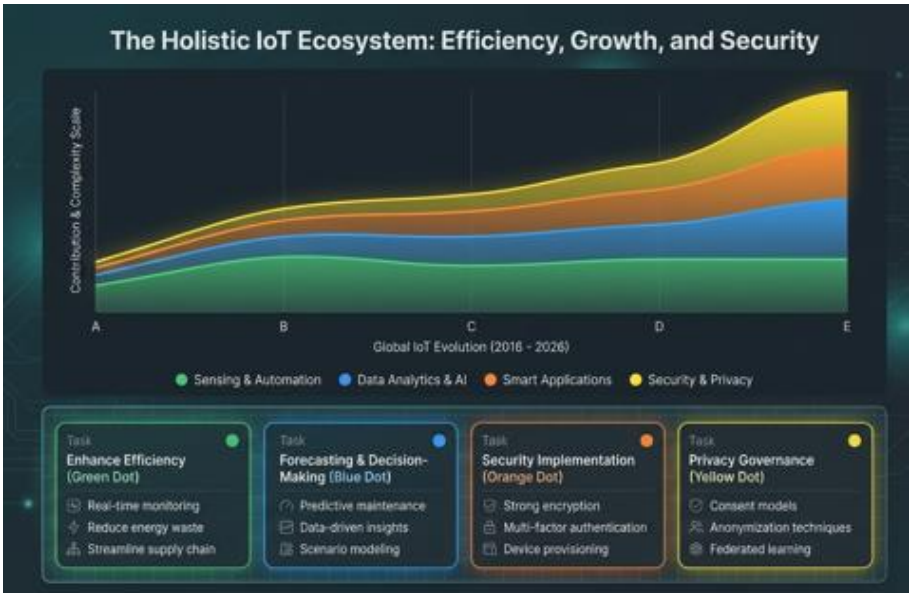


**Figure 1 9:Efficiency and growth system**

**2. Application of IOT**

Recent surveys that showcase scientific advancements across various fields have been conducted.

- We categorize current survey works into IoT goals in the ensuing subsections.
- The Internet of Things (IoT) is radically changing how we engage with the world around us.

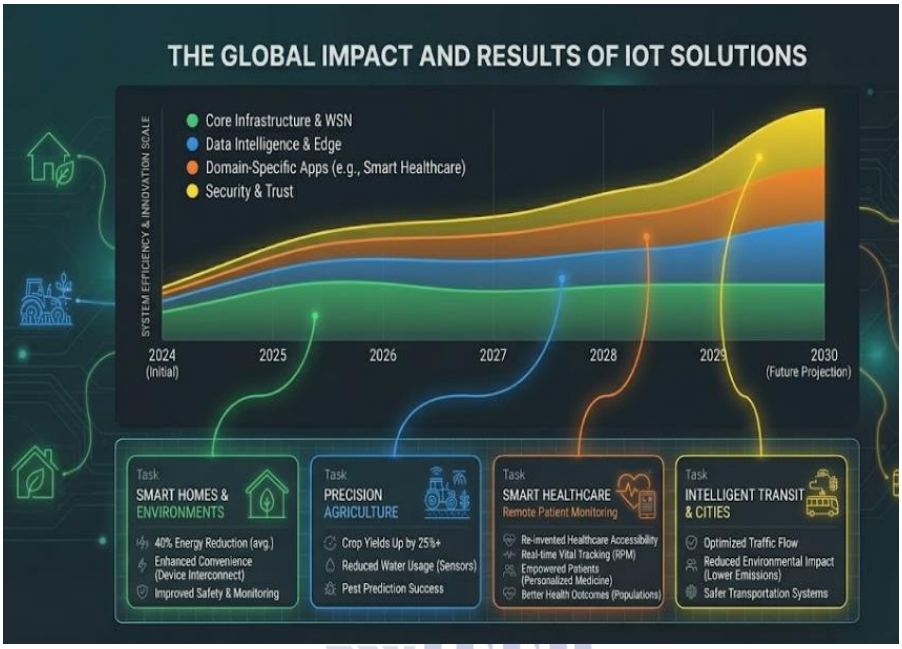


**Figure 1 10: Global Impact**

From energy-efficient and convenient smart homes to industrial settings that use predictive maintenance to simplify operations, the Internet of Things is driving innovation in every field. Precision agriculture increases agricultural crop yields, and IoT-enabled remote patient monitoring has a positive impact on the medical field. In smart cities, better traffic management leads to increased public safety.

**2.1 Motivation** Real-time data collection, analysis, and transmission are made possible by the Internet of

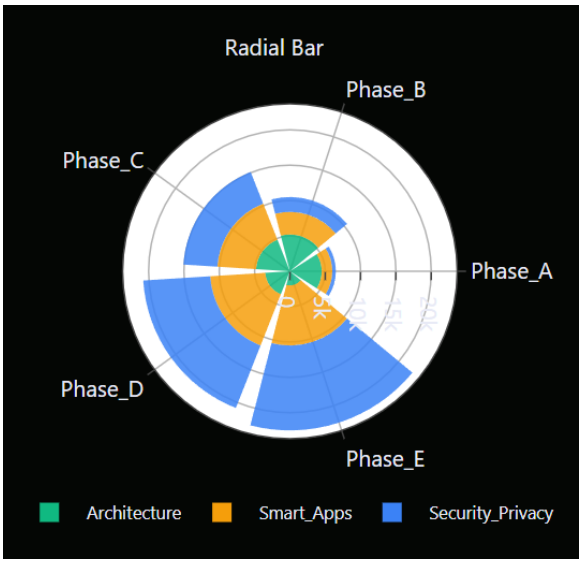


**Figure 1 11:Real time Analysis**

The enormous amount of data created and communicated by networked devices is one of the main reasons for prioritizing privacy and security in the Internet of Things. IoT systems constantly gather environmental, industrial, and personal data often without the users' knowledge. Serious privacy dangers are brought up by this, such as The growing susceptibility of IoT systems to attackers is another compelling incentive. Due to their low processing capacity and lack of integrated security mechanisms, many IoT devices are frequently used by hackers as entry points for widespread cyberthreats including ransomware, Distributed Denial of Service (DDoS) assaults, and data breaches.

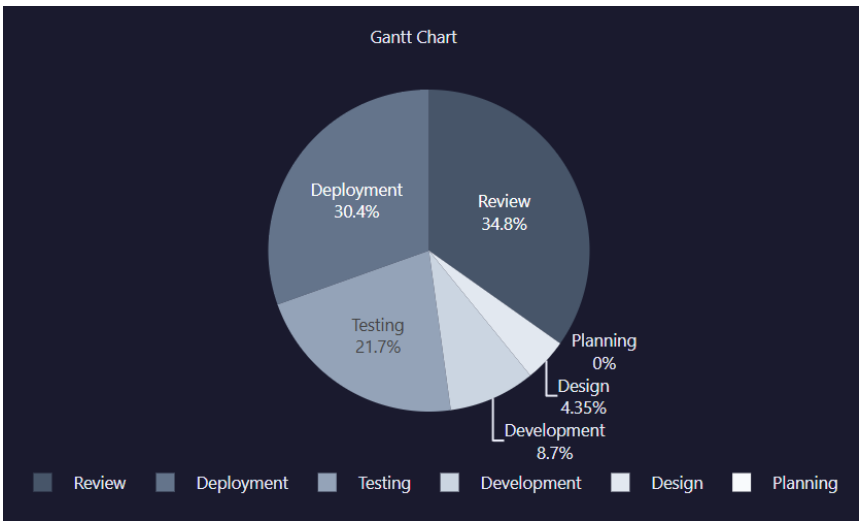


**Figure 1 12: Planning ,designing**

Smart Agriculture: Modern technology and data-driven solutions are used in precision or smart agriculture to maximize farming methods, increase crop output, and guarantee resource sustainability. By utilizing technology and analytics, smart agriculture is reorienting conventional farming methods. It can ensure agricultural sustainability for future generations while increasing food

output, reducing waste, and promoting greenery. Intelligent Houses: Smart houses use technology to improve residents' overall quality of life, comfort, security, and energy efficiency.

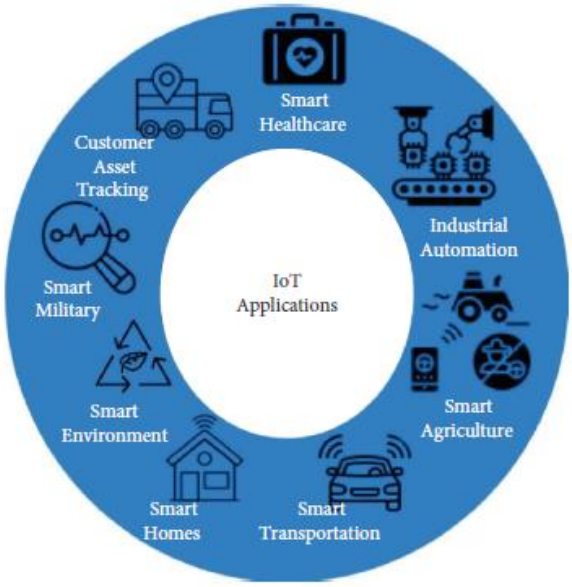


**Figure 1 13: IOT Applications**

This figure illustrates the diverse applications of the Internet of Things across multiple domains such as healthcare, smart cities, industrial automation, and agriculture. IoT enables real-time monitoring, efficient resource management, and automation through interconnected sensors and intelligent systems.

**Table 1: Smart Transportation**

| REF | AUTHORS | WORK AREA & KEY VISION |
|---|---|---|
| [1] | Oladimeji, D. | Examined smart transportation systems and their applications, focusing on the diverse technologies utilized in intelligent transport systems. |
| [8] | ResearchGate | Surveyed intelligent transportation systems using IoT, assisting in tasks like improving data propagation and creating heterogeneous connectivity. |

Table 2: Smart Agriculture

| Ref | Authors | Work Area & Key Vision |
|---|---|---|
| [17] | Quy, V.K. | Surveyed IoT solutions and demonstrated how IoT can be integrated into the smart agriculture sector. |
| [25] | ResearchGate | Explored recent developments in IoT applications within agriculture, focusing on techniques like smart drip irrigation and polyhouse monitoring. |
| [47] | Digi.com | Highlighted how IoT connects sensors, drones, and machinery to automate remote processes and provide real-time insights into soil health, weather patterns, and crop conditions. |

Table 3: Smart Military

| Ref | Authors | Work Area & Key Vision |
|---|---|---|
| [10] | Emerald Group | Revealed the use and acceptance of IoT in the military field from the view of military personnel. |
| [26] | ResearchGate | Analyzed specific areas of the application of IoT in the defense and security sector to identify possibilities of applying modern technologies in raising defense potential. |
| [33] | Kufakunesu, R. | Discussed IoT's role in enhancing military defense by connecting soldiers, vehicles, and other components, improving speed, scale, and efficiency. |

### 3. Architecture and Applications of IOT

Since there are many different technologies that make up the Internet of Things (IoT), it is impossible to create a single reference design that works for all IoT activities. There is no common IoT model since several designs are frequently combined or altered to satisfy particular system needs. An IoT architecture that guarantees simple deployment, effective data processing, and intuitive operation is ideal.

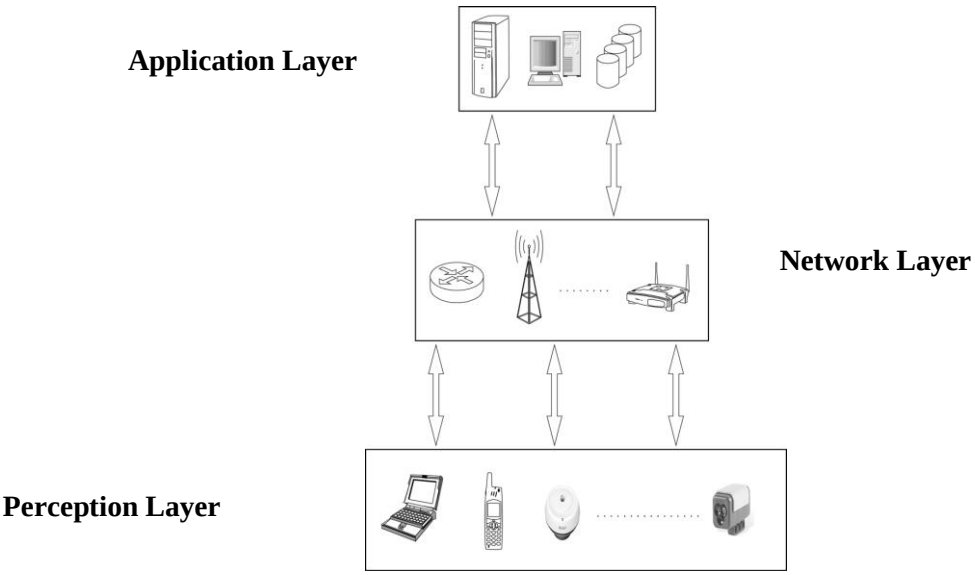


**Figure 1 14: three layer IoT architecture**

The Perception Layer collects data, the Network Layer transmits it securely, and the Application Layer provides services to users and enterprises. This layered structure enables **efficient** data collection, communication, and utilization while highlighting security and privacy considerations at each level.

1. Perception Layer: This layer is in charge of gathering information from the surroundings and recognizing tangible items. Information is sensed and collected by devices like barcode scanners, GPS modules, RFID tags, and cameras. By gathering real-world data for further processing, it serves as the cornerstone of the Internet.

2. Network Layer: The IoT system's main communication backbone is the network layer. It guarantees that information reaches the application layer safely and effectively by processing and transmitting data received from the perception layer.

All things considered, the three-layer IoT architecture provides a technical explanation of the IoT's structure.

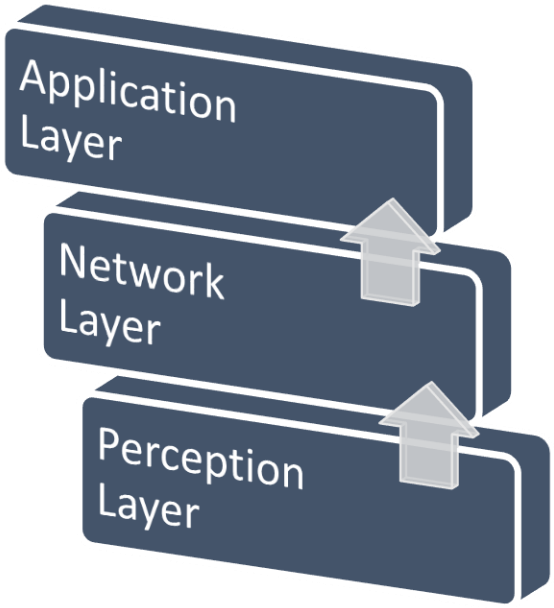


**Figure 1 15: Layered Architecture of IOT**

The Layered Architecture of the Internet of Things (IoT) explains how data flows from physical devices to applications through different layers. Each layer has a specific role that helps IoT systems work efficiently, securely, and in an organized manner.

**4. Five Architecture of IOT:** The intricate process of connecting physical objects to networks, analyzing the data they produce, and providing end users and businesses with useful insights and services is managed by the Internet of Things (IoT) architecture.


**Figure 1 16: Layers**

The Perception Layer, often referred to as the sensing layer, is the core of this architecture and is in charge of identifying and gathering information from the physical world. Sensors, actuators, RFID tags, cameras, and GPS modules make up this layer, which keeps an eye on a number of variables like temperature, humidity, motion, pressure, and position. In order to guarantee that correct and trustworthy data is sent to the upper levels, the perception layer does more than just collect data; it also carries out preparatory processing including filtering and noise reduction. The Network Layer sits above the **Perception Layer** and is in charge of sending the gathered data to processing units, cloud computing platforms, or other gadgets.

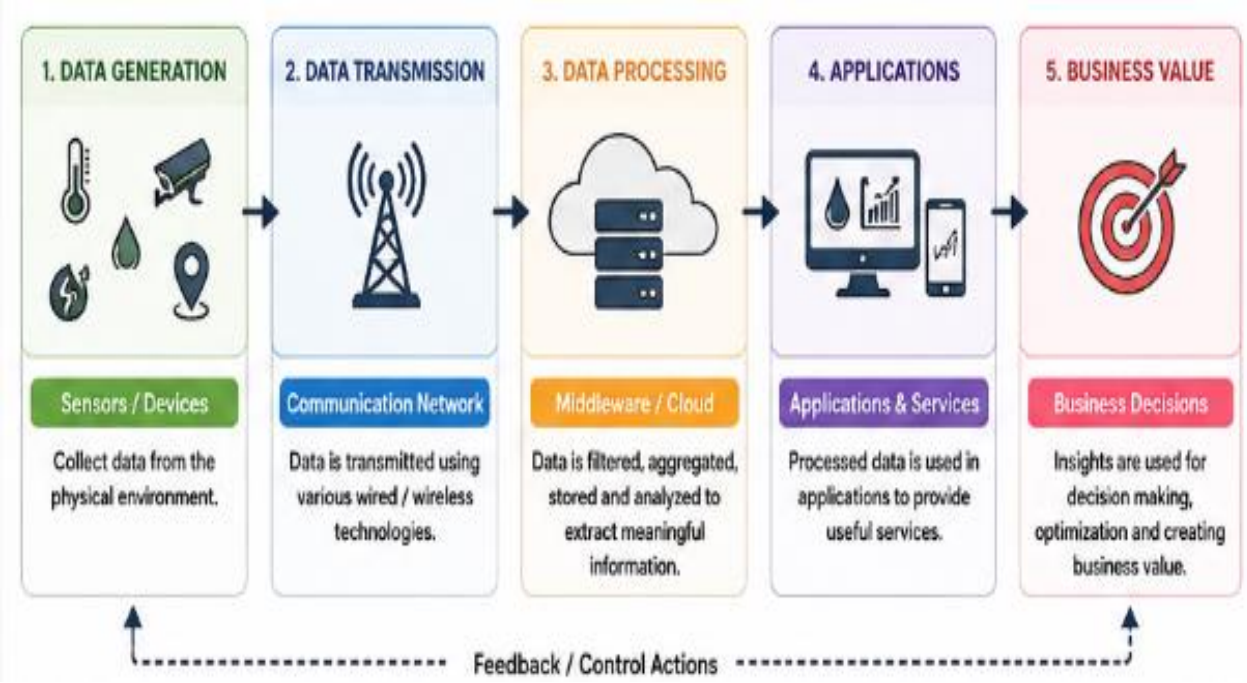


**Figure 1 17: Feedback control action**

This layer makes it possible for IoT devices to communicate with one another and guarantees that data moves across the system safely and effectively. By serving as a bridge between the network and application layers, the **middleware layer** offers crucial processing and data management functions. The raw data sent by sensors must be filtered, aggregated, and analyzed by this layer in order to be converted into information that applications and decision-making systems can use.

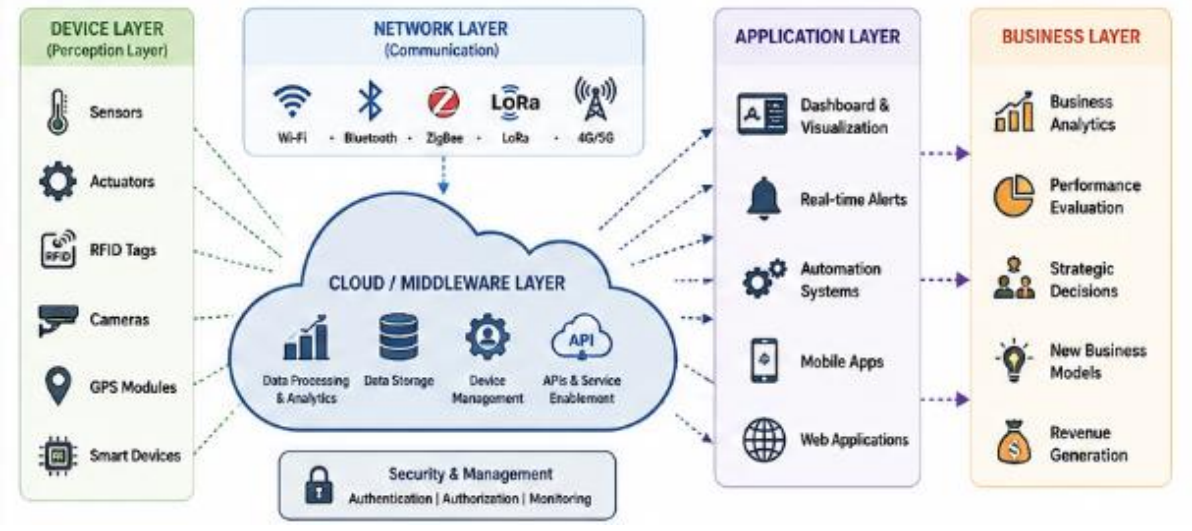


**Figure 1 18: Security Management**

It also offers application programming interfaces (APIs) that let programmers create Internet of Things apps without having to deal with the underlying hardware directly. The middleware layer provides services like edge computing, cloud storage, and real-time data processing to guarantee flexibility and compatibility. The most user-centric layer of the IoT design is the **Application Layer**, which is positioned above the middleware. It is in charge of using processed data to provide certain services to businesses, automated systems, or end consumers. The **Business Layer**, which is at the top of the architecture, is responsible for turning IoT services and data into strategic and financial value. In order to facilitate corporate decision-making, performance assessment, and the creation of new business models, this layer examines data from applications and middleware.

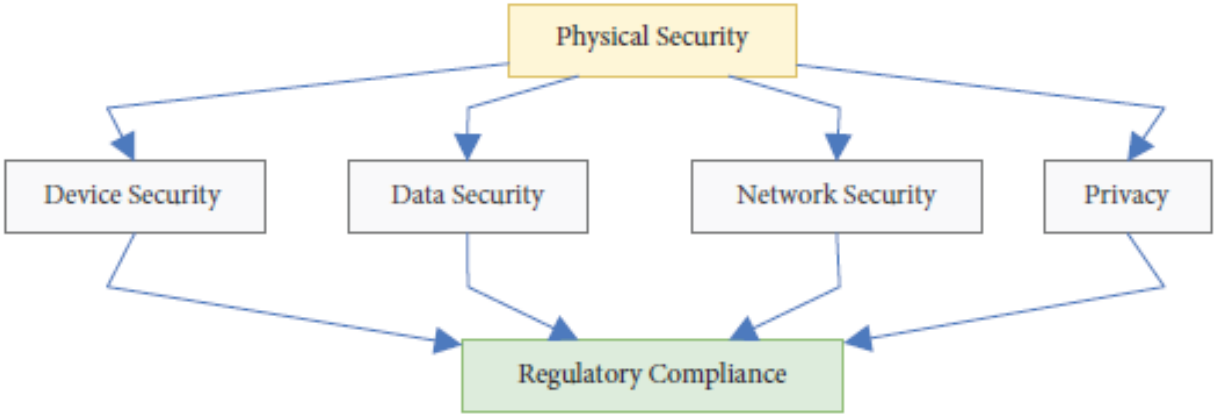


**Figure 1 19: Physical Security**

Physical Security Illustrates measures to protect IoT devices and infrastructure from unauthorized physical access, **tampering,** or environmental damage.

**6. Security and privacy Needs**

The Internet of Things (IoT) ecosystem faces significant challenges regarding security and privacy due to the limited resources of IoT devices. Traditional security suites are often too heavy for low-power devices, making it necessary to design **lightweight security frameworks** or adapt existing solutions that minimize computational and memory burdens. Security and privacy are integral to IoT, as devices continuously collect, transmit, and process sensitive user and organizational data. Without adequate protection, personal information can be exposed to unauthorized parties, and malicious actors may exploit vulnerabilities in devices or networks. Therefore, IoT systems require carefully designed mechanisms to ensure confidentiality, integrity, availability, and trustworthiness across all layers of operation.

Table 4: Authors and Technologies

| Author / Year | Key Technologies & Methods | Key Insights / Security Implications |
|---|---|---|
| [59] | Raspberry Pi, IoT sensors, industrial networks | Highlights challenges: data/service security, trust, data integrity, information privacy, scalability, interoperability. IoT integration improves monitoring but exposes devices to network attacks. |
| [60] | Cloud computing, IoT gateways, analytics platforms | Enables centralized device control and real-time data analysis. Security concern: sensitive data transmitted to cloud may be intercepted; requires encryption and authentication. |
| [61] | Edge computing, WSN, CoAP/MQTT protocols | Diverse architectures increase flexibility but require secure design principles. Highlights risk of network misconfigurations and unauthorized access. |
| [62] | Smart sensors, actuators, IoT middleware | Autonomous or semi-autonomous devices improve efficiency. Security implication: a single compromised device can disrupt operations; trust frameworks needed. |
| [63] | IoT-enabled machinery, machine-to-machine (M2M) communication | Facilitates real-time decision making and predictive maintenance. Security concern: M2M channels need robust encryption to prevent industrial espionage. |
| [64] | WSN, RFID, cloud analytics | Integrates multiple IoT technologies to monitor production lines. Key insight: data integrity and secure device authentication are critical for reliable operations. |
| [65] | IoT sensors, ML analytics, cloud platforms | IoT devices collect equipment health data for predictive maintenance. Security concern: tampered sensor data can cause wrong maintenance decisions. |
| [66] | RFID, GPS, IoT tracking | Real-time monitoring of goods in logistics reduces loss and delays. Security implications: insecure tracking devices may leak sensitive supply chain data. |
| [67] | IoT energy meters, smart grids | IoT monitors energy consumption for optimization. Vulnerabilities: energy data can reveal operational patterns; attackers may manipulate consumption data. |
| [68] | Image sensors, AI, IoT-connected cameras | Real-time quality inspection using IoT vision systems. Security concern: networked cameras must be secured to prevent data leakage or industrial sabotage. |
| [69] | IoT-enabled collaborative robots (cobots), sensors | Enhances productivity and worker safety. Security implication: compromised robots may cause physical harm or operational disruption. |
| [70] | IoT sensors for temperature, humidity, pollutants | Ensures compliance with safety and environmental standards. Vulnerabilities: tampering with sensors may lead to regulatory breaches or unsafe conditions. |
| [71] | IoT-enabled storage, RFID, automated inventory robots | Automates stock tracking and reduces human error. Security concern: compromised devices can trigger incorrect inventory records. |

## 9. Solution for IOT Security Challenges

IoT security concerns may be addressed in a variety of ways. Strong password restrictions, multi-factor authentication (MFA), certificate-based authentication, and role-based access control (RBAC) can all help to overcome weak authentication vulnerabilities and drastically cut down on unwanted access. Strict identity and

access management (IAM) regulations guarantee that only devices and people with permission may communicate inside the Internet of Things ecosystem. Additionally, implementing behavior-based access control and biometric authentication can offer an extra line of defense against credential theft and insider threats. Organizations must use secure cloud communication protocols like TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security) to guarantee data privacy and confidentiality. Lightweight cryptographic techniques that are appropriate for Internet of Things devices with constrained computing capacity should be used to encrypt all sensitive data, both in transit and at rest. The security posture of IoT installations is further reinforced by regular data handling audits, privacy impact assessments, and adherence to GDPR or ISO/IEC 27001 requirements.

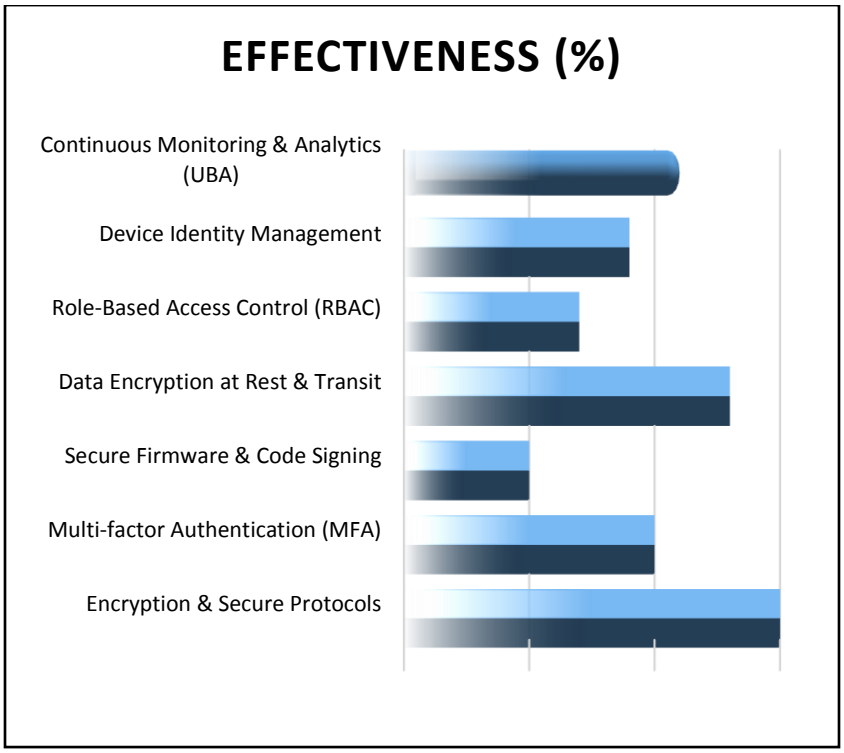


**Figure 1.20: IOT security Solutions**

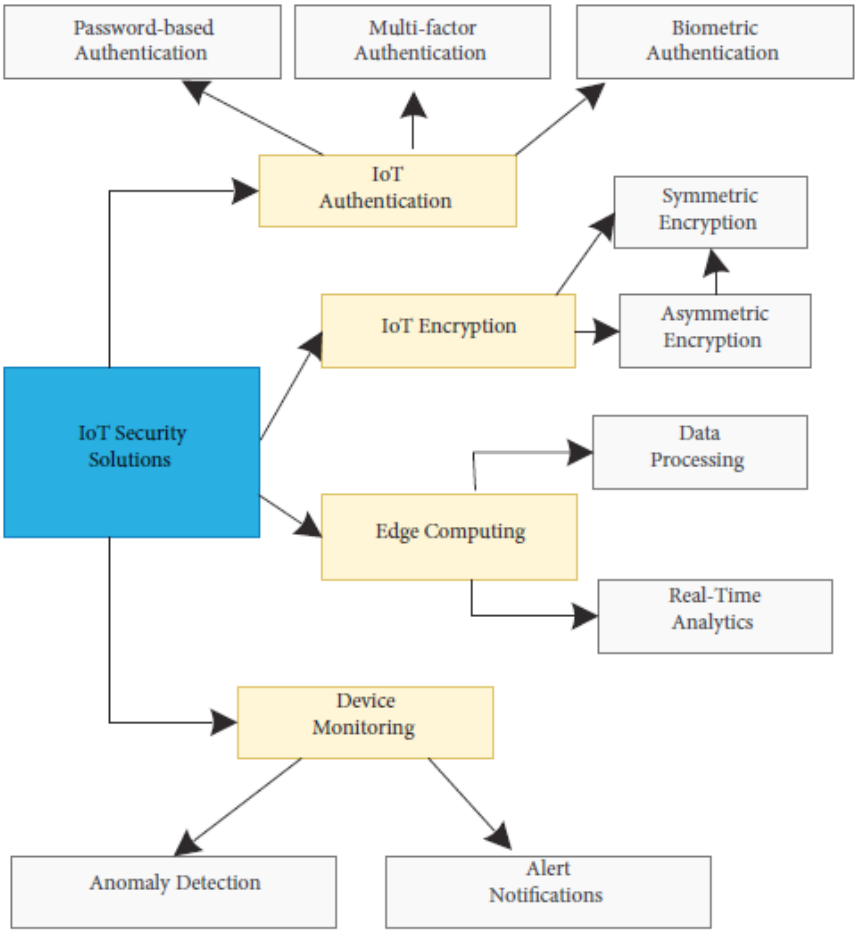


**Figure1 21: Challenges**

Solutions Depicts the comprehensive strategies to address IoT **security challenges**, including authentication, data encryption, **secure firmware updates**, and device management for a resilient ecosystem

## 10. Future Research Direction

The Internet of Things (IoT), a game-changing technology that uses sensors, networks, and intelligent algorithms to link disparate physical items, is still developing. Despite tremendous advancements, a number of research issues still need to be resolved, including those pertaining to security, privacy, interoperability, scalability, and energy efficiency. The development of flexible, intelligent, and sustainable frameworks that can manage these intricate problems in real time must be the main goal of the future generation of IoT. Integrating machine learning (ML) and artificial intelligence (AI) into Internet of Things infrastructures is one of the most exciting research avenues.

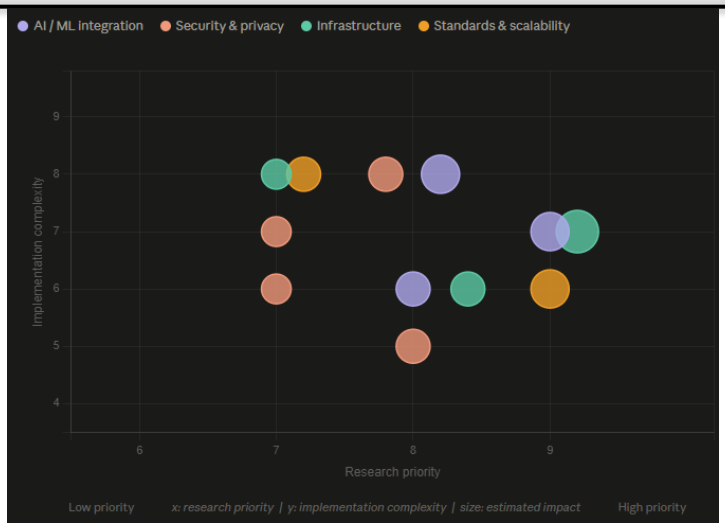


**Figure 1 22: AI/ML, Security & Privacy, Infrastructure, Standards & Scalability**

Without human assistance, AI-powered IoT devices are able to identify irregularities, understand user behavior, and improve network performance. However, integrating AI raises additional security issues that need careful consideration, such data poisoning and model manipulation.

## 11. Conclusion

With billions of devices connected and industries all over the world being transformed, the Internet of Things (IoT) has become one of the most innovative technologies of the twenty-first century. IoT facilitates data-driven decision-making, operational efficiency, and improved quality of life in a variety of contexts, including smart homes, healthcare monitoring, industrial automation, and intelligent transportation.

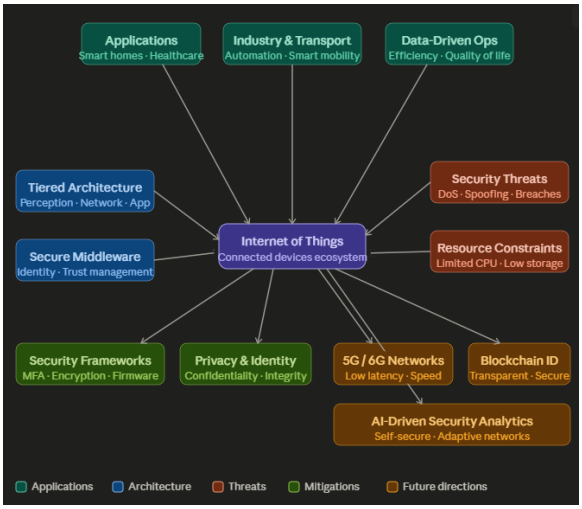


**Figure 1 23: IoT ecosystem knowledge graph: IoT conclusion ke paanch core themes (applications, architecture, threats, mitigations, future directions) aur un ke beech relationships dikhata hai. Har node clickable hai.**

But along with these enormous advantages come equally important security, privacy, scalability, and standards issues. The main uses of IoT systems, their tiered design, and important security and

privacy issues were all covered in this review study. According to the report, the Internet of Things is extremely susceptible to assaults including denial-of-service (DoS), identity spoofing, illegal access, and data breaches because of its scattered and heterogeneous nature. IoT devices are unable to handle sophisticated encryption or security suites because they frequently have limited processing power and storage. Thus, it has been determined that multi-factor authentication, data encryption, secure firmware upgrades, and lightweight security frameworks are crucial for protecting IoT settings. The significance of identity protection, trust management, and secure middleware architecture was also underlined in the conversation because these components are essential to preserving the confidentiality and integrity of data from beginning to end.

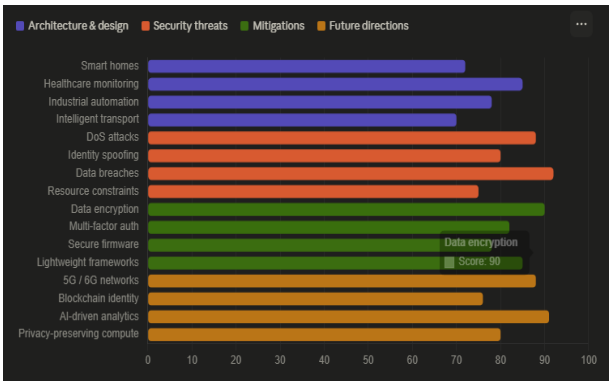


**Figure 1 24: Relative importance scores of IoT themes discussed in the conclusion (scale 0–100).**

For IoT to be successfully implemented across many industries, it is essential to manage secure communication routes, preserve user privacy, and ensure resistance to cyberattacks. The report also suggested a number of directions for further research, such as blockchain-based identity management, AI-driven security analytics, and computing methods that protect privacy. IoT networks might become self-secure, transparent, and adaptable when these cutting-edge technologies are combined. With quicker connectivity and reduced latency, the expanding use of 5G and 6G networks will further improve IoT capabilities and open up new possibilities like linked healthcare, autonomous systems, and smart.

**Reference**

Adedoyin, M. (2020). DEVELOPMENT OF A SMART IoT-BASED HOME AUTOMATION SYSTEM. Retrieved October 18, 2025, from Academia.edu website: https://www.academia.edu/download/99582100/download.pdf

Alhirabi, N., Rana, O., & Perera, C. (2021). Security and Privacy Requirements for the Internet of Things. ACM *Transactions on Internet of Things*, *2*(1), 1–37. https://doi.org/10.1145/3437537

Alrubayyi, H., Alshareef, M. S., Nadeem, Z., Abdelmoniem, A. M., & Jaber, M. (2024). Security Threats and Promising Solutions Arising from the Intersection of AI and IoT: A Study of IoMT and IoET Applications. *Future Internet*, *16*(3), 85. https://doi.org/10.3390/fi16030085

Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, Md. R. (2022). A Review of Security and Privacy Concerns in the Internet of Things (IoT). *Journal of Sensors*, *2022*(1), 1–20. https://doi.org/10.1155/2022/5724168

Azmi, A. (2020). An IoT based Home Automation Integrated Approach: Impact on Society in Sustainable Development Perspective. Retrieved October 18, 2025, from International Journal of Advanced Computer Science and Applications website: https://www.academia.edu/download/94697436/Paper_31-An_IoT_based_Home_Automation_Integrated_Approach.pdf

Belli, L., Cilfone, A., Davoli, L., Ferrari, G., Adorni, P., Di Nocera, F., ... Bertolotti, E. (2020). IoT-Enabled Smart Sustainable Cities: Challenges and Approaches. *Smart Cities*, *3*(3), 1039–1071. https://doi.org/10.3390/smartcities3030052

Butpheng, C., Yeh, K.-H., & Xiong, H. (2020). Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. *Symmetry*, *12*(7), 1191. mdpi. https://doi.org/10.3390/sym12071191

Cvar, N., Trilar, J., Kos, A., Volk, M., & Stojmenova Duh, E. (2020). The Use of IoT Technology in Smart Cities and Smart Villages: Similarities, Differences, and Future Prospects. *Sensors*, *20*(14), 3897. https://doi.org/10.3390/s20143897

Fortino, G., Savaglio, C., Spezzano, G., & Zhou, M. (2021). Internet of Things as System of Systems: A Review of Methodologies, Frameworks, Platforms, and Tools. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(1), 223–236. https://doi.org/10.1109/tsmc.2020.3042898

Garg, S., Yadav, A., Jamloki, S., Sadana, A., & Tharani, K. (2020). IoT based home automation. *Journal of Information and Optimization Sciences*, *41*(1), 261–271. https://doi.org/10.1080/02522667.2020.1721581

Garmaroodi, M. S. S., Farivar, F., Haghighi, M. S., Shoorehdeli, M. A., & Jolfaei, A. (2021). Detection of Anomalies in Industrial IoT Systems by Data Mining: Study of CHRIST Osmotron Water Purification System. *IEEE Internet of Things Journal*, *8*(13), 10280–10287. https://doi.org/10.1109/jiot.2020.3034311

Gidlund, M., Hancke, G. P., Eldefrawy, M. H., & Akerberg, J. (2020). Guest Editorial: Security, Privacy, and Trust for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *16*(1), 625–628. https://doi.org/10.1109/tii.2019.2953241

González-Zamar, M.-D., Abad-Segura, E., Vázquez-Cano, E., & López-Meneses, E. (2020). IoT Technology Applications-Based Smart Cities: Research Analysis. *Electronics*, *9*(8), 1246. https://doi.org/10.3390/electronics9081246

Gudavalli, S., & Ravi, V. K. (2024, September 20). Enhancing Data Security and Privacy in Cloud, SAP, and IoT Environments. Retrieved from Ssrn.com website: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5068395

Gupta, B. B., & Quamara, M. (2018). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, *32*(21), e4946. https://doi.org/10.1002/cpe.4946