A Comprehensive Review of IoT Systems: Architectures, Energy Efficiency, Security Frameworks, and Application Domains

[1]Kundan Kumar Pathak, [2]Arun Kumar Rai
[1]M.Tech Scholar, [2]Assistant Professor,
[1]Department of Computer Science and Engineering, Vedica Institute of Technology, Bhopal (M.P)
[2]Department of Computer Science and Engineering, Vedica Institute of Technology, Bhopal (M.P)
Email-: [1]kundan1530@gmail.com, [2]raiaruniitr@gmail.com

* Corresponding Author: Kundan Kumar Pathak

Abstract: *Connectivity has been transformed by the emergence of the Internet of Things (IoT), which allows for seamless data exchange and interaction over networks by fusing physical items with digital technology. This article emphasizes the transformative impact of IoT applications on companies and daily life by examining several elements of IoT applications across different disciplines. Critical examinations are conducted in key areas like energy optimization, security systems, IoT architecture, data frameworks, and application domains. The talk discusses the difficulties and possibilities associated with maximizing energy use, making sure security protocols are strong, organizing IoT systems, handling enormous volumes of sensor data, and deploying IoT in various industries such as waste management, smart parking, smart farming, and healthcare. The report emphasizes how crucial scalable and effective Internet of Things solutions are to promoting sustainable development and raising global standards of living.*
Keywords: Internet of Things (IoT), energy optimization, security systems, IoT architecture, data-driven frameworks, healthcare, smart farming, waste management, smart parking, connectivity, sustainability.

I. INTRODUCTION

The modern era has an internet attached to it; however, it is also essential in nature for human communication-interaction and most operational electronic devices. Thus, systems and devices are controlled and monitored remotely through this connectivity. The furtherance of high-bandwidth technologies and the consideration of different transmission media, 4G, Wi-Fi, WiMax, broadband, and so forth, have carved a good foundation for the infrastructure of IoT. A rising number of IoT devices have appeared in the recent times, owing to the fast development of technology and IT services. IoT is an enormous ecosystem of connected smart devices intended to facilitate human life. It affects numerous industries and will continue to shape how society functions toward a more connected future.The Internet of Things as stated in envisions "a world in which physical objects may become integrated into business processes and are seamlessly connected to the information network." However, through the Internet, the services could interact with the smart objects, such as accessing their status or extracting relevant data, without compromising security and privacy concerns. IoT networks, by their very nature, get complex, requiring Internet connectivity and the presence of sensor and actuators along with intelligent devices. These smart appliances and portable devices can be operational from anywhere in the world.

A. Energy Optimization

When we talk about energy optimization in IoT systems, there are three basic constituents involved: (1) behavioral improvement (2) standardization, and (3) simplified system design and efficient life cycle management. As in Figure 1, one of the first energy consumption optimization processes includes efficient life cycle management of IoT sensors. Hence energy consumed by such sensors has heavy dependency on their connected peripherals and their operational states. Power consumption [1]–[4] of these sensor nodes changes upon the life cycle stage and the data transmission strategy in use. For instance, it would consume very little energy in sleep mode while it is giving way to high consumption during data collection and transmission. So, the frequency and interval of data collection must be regulated for power efficiency of the sensors. To achieve optimal energy use-with another instance of a synonym for performance-the desired balance must be struck with the accurate data inputs. This means determining those energy thresholds for the system and then optimizing operations to those constraints[5]–[8].
The next item on the list then is, those trade-offs to reduce energy in the IoT devices should lead to a simple, effective system design. The key strategies in addressing those trade-offs include:

- Avoiding redundancy-aggregation of duplication of data and operations;
- Phasing out or reducing operational life cycle phases of sensors;
- Periodic optimization of transmission reduction-optimization of data transfer during intervals;
- Significant reduction of database algorithms-efficient management techniques for enhancing data storage;
- Simplifying the system and circuit design-lowering the complexity of the system to attain higher reliability and energy performance;
- Optimizing hardware design involves minimizing the number of components necessary for an efficient, cost-effective system.

Moreover, the IoT can contribute toward sustainability via schemes for efficient garbage collection and cost reduction by shedding unnecessary functionalities, modifying paths for data collection adaptively, and putting tools for operational optimization into the field [4]

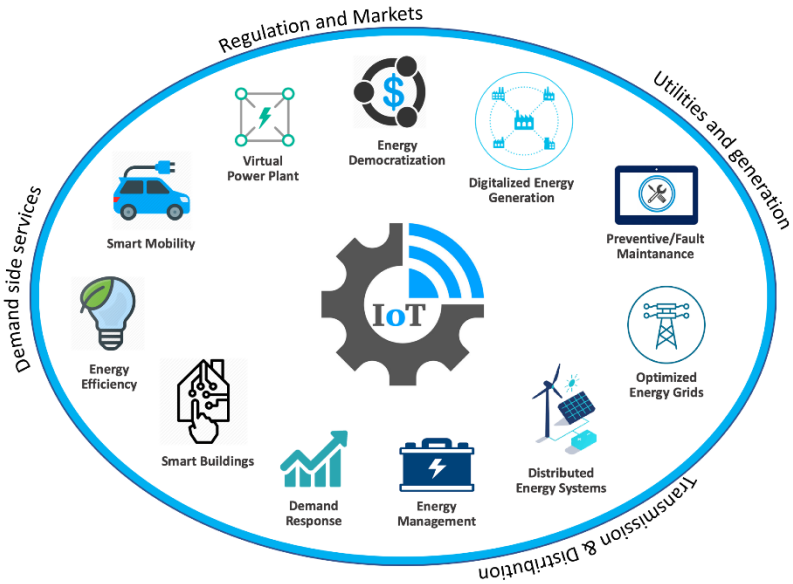

Figure 1Energy Optimization for Internet of Things [5]

B. Security System and Methods

Within an IoT ecosystem, a comprehensive security apparatus should be employed for safeguarding and ensuring the integrity of devices, data, and communication. The crucial constituents of the security framework include the security model, security bootstrapping, and network security. A security model describes how an IoT device manages its security parameters, processes, and configurations. This includes some very important practices and mechanisms: process isolation, secure storage of cryptographic keys, and enforcement of security policies. In general, the security model is expected to create a trusted operational environment by ensuring that appropriate security controls reside within the architecture of the device itself. Security bootstrapping is the initial step in securely installing a device on an IoT network because it involves the authentication and authorization of the device securely, based on time and space. During this phase, the exchange of essential security credentials and a few configuration parameters takes place in order to establish mutual trust between the device and the network. Bootstrapping is most appropriate in guaranteeing only legitimate devices gain access to the network and begin secure communications[9]–[11].

Network security is the term used for the protocols and mechanisms instituted to secure communication and activities of networked IoT devices. It tries to block access, interception, and tampering from the wrongful entities. Network security commonly ensures encryption of the data, secure routing protocols, intrusion detection and prevention systems, and control policies on access. Such processes make possible the protection of confidentiality, integrity, and availability of data within IoT environments.

Offering a wide range of components from security architecture, security models, bootstrapping procedures to network security mechanisms, one obtains a strong foundation for securing the IoT systems. Such systems aid in mitigating the threats and vulnerabilities which occur due to the interconnected nature of IoT devices and guarantee that those operations remain trustworthy and reliable[12]–[15].

C.Three-Layered IoT Architecture

Each layer within the Internet of Things (IoT) connectivity framework is defined by distinct device functionalities and operational requirements. Despite the proliferation of IoT systems over the past decade, a standardized architectural model has yet to be universally agreed upon. However, a widely accepted academic perspective categorizes IoT architecture into three core layers: the **sensor layer**, **routing layer**, and **implementation (or application) layer**. These layers collectively form the foundational structure through which IoT devices operate, communicate, and deliver value.

Sensor Layer

The sensor layer forms the first tier of the IoT architecture. It includes a wide range of sensors and actuators that interact directly with the physical environment. Sensors are responsible for detecting and measuring various parameters such as temperature, humidity, light, motion, and more. Actuators, on the other hand, perform actions in response to control

signals, enabling real-time interaction with the environment. This layer serves as the primary interface between the digital and physical worlds, capturing critical data for further processing.

Routing Layer

The routing layer manages the communication and data exchange between IoT devices. It is responsible for ensuring efficient and reliable data transmission across the network. This involves the use of optimized routing protocols and communication algorithms that determine the best path for data to travel from the source to its destination. The routing layer plays a vital role in maintaining network integrity, minimizing latency, and maximizing connectivity, especially in dynamic or large-scale IoT environments.

Implementation Layer (Application Layer)

Also known as the application layer, the implementation layer represents the highest level of IoT functionality. It encompasses the software applications, services, and tools that utilize sensor-generated data to perform specific tasks. This layer enables domain-specific solutions such as smart city infrastructures, industrial automation systems, healthcare monitoring applications, and more. By translating data into actionable insights, the implementation layer drives the practical utility of IoT systems.

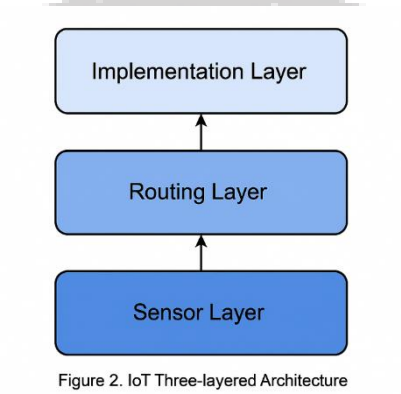

Figure 2. IoT Three-Layered Architecture

This architectural model, illustrated in Figure 2, showcases the hierarchical interaction between sensors, network communication protocols, and application-level services. It highlights the essential role each layer plays in enabling scalable, interoperable, and intelligent IoT systems.As the IoT landscape continues to expand, so too do its associated security and safety concerns. Each layer introduces unique vulnerabilities that must be addressed through robust cybersecurity strategies. Securing the IoT ecosystem is critical not only for protecting sensitive data but also for ensuring the reliable and safe operation of interconnected devices [16], [17].

II. FOUR-LAYER ARCHITECTURE FOR IOT

IoT software architecture with four layers is much more detailed than other systems. Each layer has its function and purpose so as to ensure greater operational efficiency and scalability of the system. Above this is the application layer that provides services and functionalities geared toward the user and his special domain. This layer manages and stores data in its database so data can be efficiently accessed and manipulated as required by end-users.

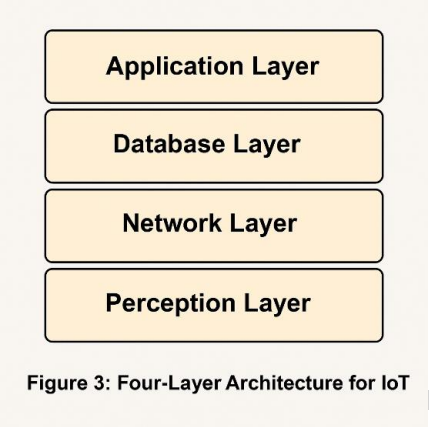

Figure 3: Four-Layer Architecture for IoT

Given in Figure 3, the application layer acts as a portal to mediate between users and the IoT system. It supports domains of smart homes, smart cities, healthcare, etc. The application layer processes meaningful information from the raw data collected by sensors to ensure that the entire IoT system accomplishes what it is intended to, accurately, and in a responsive manner.

III.DATA-DRIVEN FRAMEWORK

Typical IoT Network

The fifth generation of communications (5G) turns IoT into a dynamic and scalable platform for the collection and exchange of sensor-driven data. With the increasing complexity of connected systems, data analytics has gained enormous traction within the larger Computer Science and Engineering research community.While several strategies have been developed to improve network performance (including context-aware caching and architectural-level optimization), those focusing on data volume reduction remain separate and critical. Figure 4 shows the usual architecture of a typical IoT network, emphasizing the connected layers of sensor nodes, data aggregators, and cloud analytics.Traditionally, IoT edge nodes are burdened with low sampling rates and little processing capabilities in order to gather large volumes of data in a short time. Hence, transmission bandwidth is rarely optimized between these edge devices and central data aggregators. Nevertheless, in recent years, signal processing paradigms have been proposed to tackle this problem by means of efficient data pruning at the edge in order to reduce transmission load and latency.
Properly combined with cloud computing infrastructures, these frameworks can allow near-real-time processing of huge streams of data. Despite their hope, quite a few of these solutions aim primarily for data handling at the aggregator and control center level-rather than at first-leg collection. This fact gets more severe as IoT environments grow denser, sampling rates climb, and applications demand low-latency responses.
Given, the IoT networks must judiciously utilize computational and storage resources available at the edge and core to keep the system efficient and responsive. This double-layered approach allows the system to be scalable, inhibits unnecessary data transmissions, and performs well in delay-sensitive applications. [9], [10].

IV. CHARACTERISTICS OF IOT SENSOR DATA

IoT sensors can generate data continuously or at the instance when triggered by some external stimulus. Once detected, data is processed under certain stages, which include collection, aggregation, analysis, and visualization for the sake of deriving meaningful inferences. Usually, the inferences are taken as a direct response to the external stimulus perceived by a system. In several applications, deluge of data coming in from an IoT sensor is mixed with one or more other streams of data, which makes the hindrance even further in working with and analyzing it.
Given the scale and nature of this data, efficient aggregation, storage, and streaming mechanisms are required. These mechanisms must facilitate the efficient real-time data processing and, as well, the analysis of historical data that corresponds to varying network data rates. Nevertheless, management of IoT sensor data appears to be difficult due to its set of peculiar challenges and characteristics. Some of these challenges concern the large volumes, quick generation, timely nature, and interdependency of data sources. These sensors are embedded in human bodies, objects, or environments, which further adds physical and contextual variation.

Characteristics of IoT sensor data include:
Technical Restrictions: Small IoT sensors face limitations on computation, storage, networking, and memory usage due to their size and hardware capabilities. These limitations render them susceptible to failure, data loss, and potential malicious attacks at the data-generation stage, which, in turn, could cause interviewing with the data.
Real-Time Processing: Sensor networks must be able to process data in real time, such that the transformation of raw input into meaningful information happens instantly.

This is critical for such applications where immediate decisions and responses are required.
Scalability: Real implementations of IoT networks have numerous sensors and actuators. Scalable architectures are considered capable of coping with diverse and ever-evolving demands of IoT applications in terms of increasing data volumes and device deployments.
Data Representation: Sensor data is normally represented in compact, structured formats, such as tuples. The type of data may vary numerically, Boolean, binary, feature-based, continuous, among others, depending upon the application.
Heterogeneity: This is the main characteristic of the data supplied by the sensors of the IoT. It can stem from structured datasets, streaming data, embedded systems, social media, or participant-based sensor networks. Handling this heterogeneity guarantees the consistent integration of meaningful data.

V. APPLICATION DOMAINS OF IOT

The Internet of Things (IoT) has permeated numerous industries, transforming conventional systems into intelligent, connected ecosystems. Below are key application domains where IoT is making a significant impact:

- **Healthcare**
  IoT is revolutionizing healthcare through enhanced connectivity and real-time monitoring. Devices such as smartwatches, fitness trackers, and specialized medical sensors enable continuous health monitoring outside traditional clinical settings. These wearables can track vital signs like heart rate, blood pressure, oxygen saturation, and body temperature, alerting healthcare professionals instantly if abnormalities are detected. For example, **smart beds** in hospitals are equipped with sensors to monitor patient vitals and adjust positioning for comfort and care efficiency.
  Additionally, **Remote Patient Monitoring (RPM)** using Wireless Sensor Network (WSN) technologies allows data collection from wearable or implantable devices—such as cardiac monitors, glucometers, and respiratory sensors—enabling personalized care and timely intervention [6], [8].
- **SmartFarming**
  IoT is driving a shift toward precision agriculture by offering real-time data and automation. Farmers can deploy IoT sensors across their fields to monitor soil moisture, temperature, nutrient levels, and weather conditions. This data supports informed decisions about irrigation schedules, fertilization, and crop protection. Predictive analytics and modeling also enable optimal planting schedules, pest detection, and crop yield estimation. Ultimately, IoT in agriculture enhances productivity, improves crop quality, and reduces environmental impact through efficient resource use [7].
- **Wastemanagement**
  Conventional waste management systems often suffer from inefficiencies and high operational costs. IoT addresses these challenges by embedding sensors in waste bins to monitor fill levels in real-time. This data is transmitted to centralized systems that can dynamically schedule waste collection based on actual bin usage. Such systems reduce unnecessary collection trips, cut fuel costs, and lower emissions. Additionally, IoT-enabled waste management enhances urban cleanliness, optimizes labor allocation, and supports environmentally sustainable practices. A typical prototype involves sensors transmitting fill-level data to a cloud server, which then processes and informs workers of the required actions [11].
- **SmartParkingSystems**
  IoT-powered smart parking solutions help address the growing issue of urban parking congestion. Sensors embedded in parking spots detect vehicle presence and communicate availability to a central cloud server. Drivers can access this data via mobile applications or digital signage to locate vacant parking spaces quickly. Advanced systems even allow for space reservation and contactless payments. These innovations significantly reduce the time spent searching for parking, cut fuel consumption, and lower emissions—contributing to improved traffic flow, cleaner air, and better urban mobility [12].

VI.CONCLUSION

The Internet of Things represents an amazing technology that is changing how devices connect, communicate, and get things done---which created unprecedented opportunities for innovations in varied sectors. Energy conservation methods increase the battery life of IoT devices and, in keeping with it, enhance the working of IoT devices in large-scale deployments. Security measures are equally beneficial for protecting sensitive data, ensuring the reliability of the system, and maintaing trust in interconnected environments. The use of a structured model, such as the three-layer and four-layer architecture, has, in fact, provided a systematic method to design, implement, and manage IoT networks efficiently.
Internet of Things applications use real-time data analytics and intelligent automation for decision-making and resource optimization in healthcare, agriculture, waste management, and urban infrastructure. As IoT progresses through these steps, unlocking the potential of scalability, security, and energy-wise solutions will become increasingly key.

By meeting these demands, IoT continues to reshape technological advancement in support of a highly connected, efficient, and green future empowered with smarter user experiences.

REFERENCES

[1] Chataut R, Phoummalayvane A, Akl R. Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. Sensors. 2023; 23(16):7194. https://doi.org/10.3390/s23167194

[2] Energy Efficient Data Transmission Scheme for Internet of Things Applications Puja Banerjee, Received 21 June 2021; revised 24 April 2022; accepted 25 April 2022

[3] S. Kumar, A. Kumar, C. Gupta, and A. Chaturvedi, "Future Trends in Fault Detection Strategies for DC Microgrid," Proc. - 2024 IEEE 16th Int. Conf. Commun. Syst. Netw. Technol. CICN 2024, pp. 727–731, 2024, doi: 10.1109/CICN63059.2024.10847358.

[4] S. Kumar, A. Chaturvedi, A. Kumar, and C. Gupta, "Optimizing BLDC Motor Control in Electric Vehicles Using Hysteresis Current Controlled Boost Converters," Proc. - 2024 IEEE 16th Int. Conf. Commun. Syst. Netw. Technol. CICN 2024, pp. 743–748, 2024, doi: 10.1109/CICN63059.2024.10847341.

[5] S. Kumar, A. Kumar, C. Gupta, A. Chaturvedi, and A. P. Tripathi, "Synergy of AI and PMBLDC Motors: Enhancing Efficiency in Electric Vehicles," IEEE Int. Conf. "Computational, Commun. Inf. Technol. ICCCIT 2025, pp. 68–73, 2025, doi: 10.1109/ICCCIT62592.2025.10927757.

[6] A. Kumar and S. Jain, "Critical Analysis on Multilevel Inverter Designs for," vol. 14, no. 3, 2022, doi: 10.18090/samriddhi.v14i03.22.

[7] A. Kumar and S. Jain, "Enhancement of Power Quality with Increased Levels of Multi-level Inverters in Smart Grid Applications," vol. 14, no. 4, pp. 1–5, 2022, doi: 10.18090/samriddhi.v14i04.07.

[8] C. B. Singh, A. Kumar, C. Gupta, S. Cience, T. Echnology, and D. C. Dc, "Comparative performance evaluation of multi level inverter for power quality improvement," vol. 12, no. 2, pp. 1–7, 2024.

[9] A. Kumar and S. Jain, "Predictive Switching Control for Multilevel Inverter using CNN-LSTM for Voltage Regulation," vol. 11, pp. 1–9, 2022.

[10] C. Gupta and V. K. Aharwal, "Design of Multi Input Converter Topology for Distinct Energy Sources," SAMRIDDHI, vol. 14, no. 4, pp. 1–5, 2022, doi: 10.18090/samriddhi.v14i04.09.

[11] C. Gupta and V. K. Aharwal, "Design and simulation of Multi-Input Converter for Renewable energy sources," J. Integr. Sci. Technol., vol. 11, no. 3, pp. 1–7, 2023.

[12] C. Gupta and V. K. Aharwal, "Optimizing the performance of Triple Input DC-DC converter in an Integrated System," J. Integr. Sci. Technol., vol. 10, no. 3, pp. 215–220, 2022.

[13] A. Kumar and S. Jain, "Multilevel Inverter with Predictive Control for Renewable Energy Smart Grid Applications," Int. J. Electr. Electron. Res., vol. 10, no. 3, pp. 501–507, 2022, doi: 10.37391/IJEER.100317.

[14] V. Meena and C. Gupta, "A Review of Design , Development , Control and Applications of DC − DC Converters," no. 2581, pp. 28–33, 2018.

[15] A. K. Singh and C. Gupta, "Controlling of Variable Structure Power Electronics for Self-Contained Photovoltaic Power Technologies," vol. 05, no. 02, pp. 70–77, 2022.

[16] A. Hridaya and C. Gupta, "Hybrid Optimization Technique Used for Economic Operation of Microgrid System," Academia.Edu, vol. 5, no. 5, pp. 5–10, 2015, [Online]. Available: http://www.academia.edu/download/43298136/Aditya_pape_1.pdf.

[17] S. Khan, C. Gupta, and A. Kumar, "An Analysis of Electric Vehicles Charging Technology and Optimal Size Estimation," vol. 04, no. 04, pp. 125–131, 2021.

[18] S. Kumar and A. Kumar, "Single Phase Seventeen Level Fuzzy-PWM Based Multicarrier Multilevel Inverter with Reduced Number of Switches."

[19] P. Verma and M. T. Student, "Three Phase Grid Connected Solar Photovoltaic System with Power Quality Analysis," pp. 111–119, 2018.

[20] Kothandaraman, D., Balasundaram, A., Dhanalakshmi, R., Sivaraman, A. K., Ashokkumar, S., Vincent, R., & Rajesh, M. (2022). Energy and Bandwidth Based Link Stability Routing Algorithm for IoT. Computers, Materials & Continua, 70(2).

[21] Almalki, F. A., Alsamhi, S. H., Sahal, R., Hassan, J., Hawbani, A., Rajput, N. S., ... & Breslin, J. (2023). Green IoT for eco-friendly and sustainable smart cities: future directions and opportunities. Mobile Networks and Applications, 28(1), 178-202.

[22] Thai, H. T., Nguyen-Tran, T. L., & Le, K. H. (2022, October). Toward a predictive smart parking system in IoT-enabled cities. In 2022 9th NAFOSTED Conference on Information and Computer Science (NICS) (pp. 1-6). IEEE.