International Journal of
Distributed Computing and Technology

ISSN: 2455-7307
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJDCT

https://journalspub.com/journal/ijdct/

Review IJDCT

Fog Computing Architecture and Deployment in IoT

Kazi Kutubuddin Sayyad Liyakat*

Abstract

The relentless proliferation of Internet of Things maneuvers generates colossal volumes of data at the network edge, straining traditional cloud-centric paradigms with inherent limitations in latency, bandwidth, resilience, and privacy. This necessitates a paradigm shift towards distributed intelligence. Fog Computing arises as a pivotal architectural paradigm, extending computational, storage, and networking capabilities closer to the data source, thereby mitigating latency, reducing bandwidth consumption, and enhancing real-time processing capabilities for critical IoT applications. This paper delves into the foundational architecture of Fog Computing, dissecting its intricate layering from diverse edge devices (sensors, actuators, and gateways) through intermediate Fog nodes (routers, switches, and micro-data centers) to the overarching cloud hierarchy. We analyze key design principles, including geographical distribution, heterogeneity, virtualization, and the interplay between local and global intelligence. Furthermore, we examine critical considerations for its effective deployment in diverse IoT verticals, addressing challenges such as dynamic resource orchestration, energy efficiency, interoperability, robust security protocols across heterogeneous environments, and the need for standardized management frameworks. By exploring both the theoretical underpinnings and practical implications, this work underscores Fog Computing's transformative potential to unlock new frontiers in intelligent, responsive, and resilient IoT ecosystems, paving the way for truly autonomous and data-driven decision-making at the edge.

Keywords: Fog computing, Internet of Things (IoT), architecture and deployment, management, geographical distribution, intrusion detection systems

INTRODUCTION

Internet of Things (IoT) is a symphony of data, a constant hum of sensors and devices generating information at an ever-increasing pace. Yet, as this symphony swells, the traditional reliance on distant, centralized cloud servers begins to feel like shouting across a vast, echoey hall. The latency, bandwidth constraints, and potential single points of failure become glaring limitations. Enter fog computing, not as a replacement for the cloud, but as its whispering, intelligent neighbor – closer to the source, more agile, and intimately aware of the real-time needs of the IoT [1].

***Author for Correspondence**
Kazi Kutubuddin Sayyad Liyakat
E-mail: drkkazi@gmail.com

Professor and Head, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

Received Date: October 29, 2025
Accepted Date: November 02, 2025
Published Date: December 23, 2025

Citation: Kazi Kutubuddin Sayyad Liyakat. Fog Computing Architecture and Deployment in IoT. International Journal of Distributed Computing and Technology. 2025; 11(2): 31–39p.

Imagine a world where your smart thermostat doesn't just send temperature readings to the cloud, but processes them locally, adjusting your HVAC system in milliseconds based on your presence and learned habits. Or where a fleet of autonomous vehicles can share immediate hazard alerts and coordinate maneuvers without waiting for a round trip to a distant data center. This is the promise of fog computing [2].

At its core, fog computing architecture is about distributing computational, storage, and networking properties closer to the edge of the network, where

the IoT devices reside. This creates a multitiered hierarchy, often visualized as a "fog plane" nestled between the devices and the cloud [3].

Here's a Breakdown of the key Architectural Components:

- *IoT Devices (The Endpoints):* These are the originators of data – sensors, actuators, smart appliances, wearables, and industrial machinery. They are the "leaves" of the network, generating the raw information.
- *Edge Nodes (The First Responders):* This is where the fog truly begins to form. Edge nodes are devices with enhanced processing power and storage capabilities located very close to the IoT devices. Think smart gateways, industrial personal computers (PCs), small servers on factory floors, or even sophisticated routers. They are responsible for:
  - *Data Filtering and Preprocessing:* Sifting through the torrent of raw data to extract actionable insights and discard noise.
  - *Local Analytics and Decision-Making:* Performing real-time analysis and executing immediate responses without cloud intervention.
  - *Protocol Translation:* Bridging communication gaps between diverse IoT devices and the broader network.
  - *Security Enforcement:* Implementing local security measures and access control.
- *Fog Nodes (The Middle Managers):* These are more robust computing resources situated at the "edge of the edge" – perhaps at local offices, cellular towers, or aggregation points within a campus. They offer:
  - *Aggregated Data Processing:* Handling data from multiple edge nodes, performing more complex analytics and pattern recognition.
  - *Short-Term Data Storage and Caching:* Retaining historical data for faster local retrieval and trend analysis.
  - *Application Hosting:* Deploying lightweight, latency-sensitive applications that benefit from proximity.
  - *Coordination and Orchestration:* Managing and directing the activities of multiple edge nodes.
- *Cloud (the Central Brain):* While the fog handles immediate needs, the cloud remains crucial for.
  - *Long-Term Data Storage and Archiving:* Storing vast datasets for historical analysis, compliance, and big data insights.
  - *Deep Learning and Advanced Analytics:* Training complex machine learning (ML) models that need noteworthy computational power.
  - *Global Data Aggregation and Management:* Providing a unified view and control over distributed IoT deployments.
  - *System-Wide Updates and Orchestration:* Managing the overall control plane and deploying updates to fog and edge nodes.

KEY ARCHITECTURAL PRINCIPLES THAT DEFINE THE FOG

- *Proximity:* Resources are placed physically closer to the data source.
- *Distribution:* Computational power is spread across multiple points, not concentrated in a single location.
- *Heterogeneity:* Fog architecture often includes a mix of diverse software and hardware platforms.
- *Interoperability:* Seamless communication and data exchange between different tiers are paramount.
- *Real-Time Capabilities:* The ability to process data and respond with minimal latency is a defining characteristic.
- *Deploying the Fog:* Bringing intelligence to the edge.

The deployment of fog computing in IoT is not a one-size-fits-all affair. It requires careful reflection of the specific application, its latency requirements, data volume, security needs, and existing infrastructure. Here are common deployment strategies.

- *Industrial IoT (IIoT):* In factories and manufacturing plants, edge nodes can be industrial PCs and gateways that collect data from machines, perform real-time quality control checks, predict equipment failures, and optimize production processes. Fog nodes might be servers located in a local control room or a nearby facility.
- *Smart Cities:* Traffic management systems can deploy edge nodes in traffic lights to analyze vehicle flow and adjust timings dynamically. Smart grid systems can use fog nodes to monitor energy consumption at a local level and respond to fluctuations. Public safety applications can leverage edge devices for real-time video analytics.
- *Healthcare:* Wearable health monitors can process vital signs locally (edge), alerting users and potentially healthcare providers to immediate anomalies. Fog nodes in hospitals or clinics could aggregate data from multiple patients for faster diagnosis or localized treatment adjustments.
- *Smart Homes:* Smart thermostats, etc., act as edge devices, processing commands and basic analytics locally. A dedicated home gateway could serve as a fog node, orchestrating these devices and providing faster response times.
- *Autonomous Vehicles:* Vehicles themselves are powerful edge computing platforms, processing sensor data for navigation and immediate decision-making. Vehicle-to-vehicle and vehicle-to-infrastructure communication, facilitated by roadside fog nodes, enables cooperative driving and enhanced safety.

CHALLENGES AND CONSIDERATIONS IN DEPLOYMENT

- *Resource Management:* Efficiently allocating and managing computational, storage, and network resources across a distributed fog infrastructure can be complex.
- *Security and Privacy:* Protecting data at multiple distributed points becomes more challenging. Robust security protocols and encryption are essential.
- *Interoperability and Standardization:* Safeguarding seamless communiqué and data exchange among diverse hardware and software components from different vendors is crucial.
- *Orchestration and Management:* Developing sophisticated tools and platforms to deploy, monitor, and manage the distributed fog environment is a significant undertaking.
- *Scalability:* The fog architecture must be designed to scale efficiently as the number of IoT devices and data volumes grow.
- *Cost:* While fog computing can reduce cloud costs, the initial investment in edge and fog hardware and infrastructure needs to be justified.

Fog computing is not a fleeting trend; it's an evolutionary step in the IoT landscape. By bringing intelligence closer to the source, it unlocks a new era of responsive, efficient, and truly intelligent connected systems. As the IoT continues its relentless expansion, the whispering edge of fog computing will become increasingly vital, ensuring that the symphony of data it generates is not just heard but understood and acted upon with unparalleled speed and precision. The future of connected devices is not solely in the distant cloud, but in the responsive, ever-present intelligence of the fog [4].

FOUNDATIONAL ARCHITECTURE AND DEPLOYMENT OF FOG COMPUTING

The explosion of IoT – billions of sensors, devices, and actuators generating continuous streams of data – has created an architectural imperative. While the Cloud reigns supreme for ultimate storage and deep analytics, it struggles under the sheer weight and velocity of real-time data flow. Latency, bandwidth restrictions, and the need for immediate, localized decision-making require a different approach [5].

This is the domain of Fog Computing: the essential middle layer that extends the power of the Cloud closer to where the data is generated. Fog is not intended to replace the Cloud, but to act as the spinal cord of the IoT ecosystem, managing immediate reflexes and aggregating information before relaying critical summaries to the brain [6].

The defining characteristics of modern IoT applications – especially in fields, like IIoT, smart cities, and autonomous systems – demand processing speeds far exceeding what traditional centralized Cloud architecture can provide.

The Latency Problem

For mission-critical applications (e.g., controlling a robotic arm in a factory, or applying brakes in an autonomous vehicle), time is measured in milliseconds. Relaying raw data thousands of miles to a central server for processing introduces unacceptable latency. Fog nodes perform real-time local analytics, enabling immediate responses without relying on the network backhaul.

Bandwidth and Data Overload

A single industrial plant can generate petabytes of data daily. Pushing all this raw data to the Cloud is prohibitively expensive and inefficient. Fog nodes act as sophisticated data filters, aggregating, scrubbing, and summarizing the data, sending only the most crucial insights upstream. This dramatically reduces the required bandwidth.

Resilience and Security

By distributing processing power, Fog architecture enhances system resilience. If the network connection to the central Cloud fails, local operations can continue processing critical tasks independently. Furthermore, Fog nodes can enforce security policies and conduct initial anomaly detection right at the edge, isolating threats before they can spread.

Foundational Architecture: The Three Layers

Fog computing inherently defines a continuum of compute power, differentiating itself from the simple two-layer (Edge and Cloud) model. Its architecture is typically conceptualized across three interconnected strata:

Layer 1: The Edge (The Things Layer)

This is the lowest stratum, composed of end-devices: sensors, actuators, cameras, wearables, and microcontrollers. These devices are generally low-power, resource-constrained, and focused purely on data collection and actuation. They perform minimal, if any, processing beyond basic filtering.

Layer 2: The Fog (The Compute and Control Layer)

The Fog layer is the core of architecture. It consists of high-performance gateways, routers, dedicated servers, and access points physically located near or within the network premises (e.g., factory floor, cellular tower base stations).

Key Functions of Fog Nodes

- *Data Ingestion and Aggregation:* Collecting data from hundreds or thousands of Edge devices.
- *Stream Processing:* Performing complex analysis on data streams in motion (e.g., running ML inference models, identifying threshold breaches).
- *Local Decision Making:* Executing control loops and automated responses without Cloud intervention.
- *Protocol Translation:* Standardizing data formats received from heterogeneous Edge devices before sending them upstream.
- *Temporary Storage:* Caching critical data for short-term analysis or resilience during network outages.

Layer 3: The Cloud (The Global and Historical Layer)

This highest stratum handles tasks requiring massive, long-term computational resources. The Cloud is responsible for global coordination, historical data warehousing, high-level business intelligence, and resource-intensive tasks, such as training sophisticated AI models, that are then distributed back down to the Fog nodes for local execution (inference).

Deploying robust Fog architecture requires strategic placement of compute resources and a flexible management framework that can handle the massive physical distribution of nodes.

Fog Node Hardware and Placement

Unlike centralized data centers, Fog nodes are physically dispersed and often ruggedized to survive harsh environments (e.g., extreme temperatures in a warehouse or outdoor smart city environment).

- *Gateways:* The most common Fog deployment, gateways act as the initial collection point, running containerized applications (like Docker or Kubernetes) to execute real-time analytics.
- *Micro-Data Centers:* In large IIoT environments, dedicated, powerful servers (sometimes called "Mist Nodes" when resources are very constrained) are deployed on-site to provide robust local processing power – essentially bringing a portion of a data center closer to the action.

The Management Plane: Orchestration and Security

The greatest challenge in Fog deployment is managing thousands of distributed, heterogeneous nodes. This requires a robust orchestration layer as revealed in Table 1.

Table 1. Challenges in Fog deployment.

Mechanism	Description
Containerization	Using lightweight technologies (like Docker or specialized Edge containers) to package and deploy applications consistently across diverse Fog hardware.
Decentralized control	Management systems must be able to push configuration updates, security patches, and new AI models from the Cloud down to the specific Fog nodes, often autonomously.
Zero-trust security	Because Fog nodes exist outside the traditional security perimeter of a data center, every node and every data packet must be authenticated and authorized, requiring robust public-key infrastructure and granular access controls distributed across the network.

Data Flow and Feedback Loops

The deployment is defined by the flow of information

- *Ingress:* Raw data flows from the Edge (sensors) to the Fog node.
- *Processing:* The Fog node executes local analytics (fast inference). Immediate actions are sent back down to the Edge (actuators).
- *Egress:* Summarized, filtered, and aggregated data flows up to the Cloud for long-term storage and training.
- *Feedback or Training:* Newly trained models or global insights are pushed down from the Cloud to the Fog nodes, continuously improving local intelligence.

Fog computing is not merely an architectural novelty; it is the fundamental necessity for realizing true intelligence at scale in IoT.

In smart cities, Fog nodes installed on traffic lights and utility poles enable instantaneous adaptive traffic control and rapid response to localized emergencies. In healthcare, Fog nodes within hospitals process real-time patient monitoring data, triggering alerts faster than centralized systems, potentially saving lives [7].

Ultimately, the foundational architecture of Fog computing decentralizes intelligence, democratizes real-time decision-making, and guarantees the speed and resilience required for the next generation of mission-critical interconnected systems. It is the architectural linchpin connecting the passive world of sensors to the boundless power of the Cloud [8].

UNVEILING FOG COMPUTING'S DESIGN PRINCIPLES FOR AN IOT-DOMINATED WORLD

IoT is no longer a futuristic concept; it's the pulsating digital heartbeat of our modern world. From smart cities to autonomous vehicles, connected devices are generating an unprecedented deluge of data.

Yet, the traditional model of sending every byte to a distant cloud for processing quickly falters under the weight of latency, bandwidth constraints, and security risks. Enter fog computing – the intelligent haze that bridges the gap between the data-generating edge and the powerful, but distant, cloud. It's not a replacement for the cloud, but rather its indispensable partner, extending compute, storage, and networking closer to where the action happens [9].

To understand Fog's transformative power, we must delve into its core design principles – the architectural pillars that enable it to unlock the true potential of IoT deployments.

The Bedrock of Edge Intelligence: Key Design Principles

- *Proximity and Low Latency:* This is Fog's defining characteristic. By pushing computational power, storage, and application services to the "edge" – closer to IoT devices – Fog dramatically reduces the time it takes for data to travel, be processed, and for an action to be initiated. For critical IoT applications, like autonomous driving, industrial automation, or remote surgery, millisecond differences can be catastrophic. Fog ensures near real-time responsiveness, enabling immediate decision-making at the source [10].
- *Geographical Distribution:* Unlike the centralized nature of cloud data centers, Fog nodes are inherently spread out, mirroring the distributed nature of IoT devices themselves. They can be found in smart traffic lights, factory floor gateways, cellular base stations, or even within vehicles. This wide dispersion allows for localized data processing, reducing the burden on core networks and catering to the diverse physical locations of IoT deployments.
- *Hierarchy and Layered Architecture:* Fog computing isn't flat; it's a multilayered ecosystem. It often forms a continuum from the very edge devices (sensors, actuators) to fog nodes (gateways, routers, specialized servers), and finally up to the distant cloud. This hierarchy allows for intelligent data filtering and aggregation. Only processed, actionable insights, or aggregated raw data, need to traverse up the chain, optimizing bandwidth and storage at higher tiers [11].
- *Heterogeneity:* The IoT landscape is a wild jungle of diverse devices, operating systems, communication protocols (Wi-Fi, Bluetooth, LoRaWAN, and 5G), and data formats. A key principle of Fog is its ability to embrace and manage this heterogeneity. Fog nodes are designed to be protocol-agnostic, capable of interfacing with a wide array of devices and translating data formats, acting as a crucial interoperability layer.
- *Interoperability and Standardization (Emerging):* While heterogeneity is embraced, the ability for different fog nodes from various vendors to communicate and collaborate seamlessly is paramount. Emerging standards and APIs are crucial for building cohesive fog ecosystems, allowing for the sharing of resources, data, and services across different fog deployments and between fog and cloud layers.
- *Security and Privacy:* Processing sensitive data closer to its source presents unique security challenges and opportunities. Fog architectures prioritize distributed security mechanisms, including localized encryption, access control, anomaly detection at the edge, and even localized data anonymization. This minimizes the exposure of raw, sensitive data to the broader network and allows for adherence to data sovereignty regulations by keeping data within specific geographical boundaries.
- *Scalability and Flexibility:* As the number of IoT devices and applications grows, the Fog architecture must be able to scale efficiently. New fog nodes should be easily added or removed, and their resources dynamically allocated. This flexibility ensures that the system can adapt to evolving demands without requiring a complete overhaul.
- *Autonomy and Self-Organization:* Fog nodes, to some extent, possess autonomy. They can make local decisions, execute tasks, and even collaborate with nearby nodes without constant supervision from the cloud. This self-organizing capability enhances resilience, allowing operations to continue even if connectivity to the central cloud is temporarily lost.

The deployment of Fog computing transforms theoretical principles into tangible benefits across numerous IoT sectors.

- *Smart Cities:* Fog nodes in traffic lights can analyze real-time traffic flow to optimize signal timing, reducing congestion and emissions without sending continuous video streams to the cloud. Public safety cameras can perform on-device object detection, alerting authorities only to unusual events.
- *IIoT:* In smart factories, fog gateways can monitor machine health, detect anomalies, and trigger predictive maintenance alerts instantaneously, preventing costly downtime. Real-time control loops for robotic arms or assembly lines can reside on local fog nodes for ultra-low latency and precision.
- *Healthcare:* Wearable health devices can offload initial processing of vital signs to a home fog gateway, sending only critical alerts or aggregated data to medical professionals, enhancing privacy and reducing network load for continuous monitoring.
- *Autonomous Vehicles:* Processing sensor data from LiDAR, cameras, and radar requires immense computational power and near-zero latency. Fog nodes within the vehicle and at roadside units enable real-time decision-making for navigation, collision avoidance, and traffic management, crucial for safety [12].
- *Agriculture:* Precision farming uses fog nodes on tractors or in fields to analyze soil conditions, weather patterns, and crop health in real-time, optimizing irrigation and fertilization, leading to higher yields and reduced resource consumption.

Fog computing is not merely an optimization; it's a fundamental paradigm shift that empowers the IoT. By embedding intelligence, computing, and decision-making capabilities closer to the data source, it addresses the inherent limitations of cloud-only architectures. As the IoT continues its exponential growth, stretching the boundaries of our digital infrastructure, the intelligent haze of Fog computing will undoubtedly consolidate its position as a cornerstone technology, orchestrating a more responsive, efficient, secure, and truly intelligent connected world. The future of IoT isn't just in the cloud; it's profoundly rooted in the capabilities of the intelligent edge.

CRITICAL CONSIDERATIONS FOR THE EFFECTIVE DEPLOYMENT OF FOG COMPUTING IN IOT

The rapid proliferation of IoT has necessitated a shift from traditional cloud-centric architectures to more distributed computing paradigms. Fog computing, positioned between IoT devices and centralized cloud servers, offers a compelling solution by enabling real-time processing, reducing latency, and optimizing bandwidth usage. However, deploying fog computing infrastructure effectively in IoT applications requires careful consideration of several critical factors.

Latency and Real-Time Processing Requirements

The primary motivations for adopting fog computing are the need for low-latency responses in applications like industrial automation and healthcare monitoring. Critical systems require fog nodes to be strategically placed close to data sources to minimize delays.

- *Response Time Analysis:* Determine acceptable latency thresholds for each application.
- *Dynamic Workload Allocation:* Distribute computation tasks efficiently between edge, fog, and cloud layers.

Scalability and Resource Management

Fog computing environments must dynamically scale to accommodate increasing IoT device loads without performance degradation.

- *Node Distribution:* Ensure fog nodes are deployed in a hierarchical fashion to balance computational loads.
- *Elastic Resource Provisioning:* Utilize virtualization and containerization technologies (e.g., Docker, Kubernetes) to manage resource allocation dynamically.

- *Load Balancing Algorithms:* Implement adaptive strategies to prevent node overloading.

Security and Privacy Alarms

Fog computing presents new security challenges due to its distributed nature. With data processing occurring at multiple points, attack surfaces expand, necessitating robust security measures.

- *Authentication and Authorization:* Implement secure identity management and role-based access control.
- *Data Encryption:* Secure data in transit (TLS) and at rest (AES).
- *Intrusion Detection Systems (IDS):* Deploy anomaly-based monitoring at fog nodes to detect malicious activities.
- *Compliance with Regulations:* Ensure adherence to GDPR, HIPAA, or industry-specific data protection laws.

Network Reliability and Bandwidth Optimization

Fog computing mitigates cloud dependence by processing data locally, but network reliability remains critical.

- *Redundancy and Failover Mechanisms:* Ensure high availability by deploying backup fog nodes.
- *Data Filtering and Compression:* Reduce unnecessary data transmission to the cloud.
- *5G and Edge Integration:* Leverage high-speed, low-latency networks for seamless fog-cloud communication.

Interoperability and Standardization

IoT ecosystems consist of heterogeneous devices and protocols. Successful fog deployments must ensure seamless interoperability.

- *Adoption of Open Standards:* Utilize frameworks like OpenFog (IEEE 1934) and IIoT standards.
- *API-Based Communication:* Enable cross-platform integration via RESTful APIs or MQTT protocols.

Energy Efficiency and Sustainability

Fog nodes, particularly in remote or battery-powered IoT applications, must operate efficiently to prolong system longevity.

- *Low-Power Hardware:* Employ energy-efficient processors (e.g., ARM-based architecture).
- *Task Offloading Strategies:* Balance energy consumption between devices and fog nodes.

Cost-Effectiveness and ROI Considerations

While fog computing reduces cloud dependency, deploying and maintaining fog infrastructure entails costs.

- *Capex versus Opex Analysis:* Assess whether self-hosted fog nodes or managed fog services (e.g., AWS Greengrass, Azure IoT Edge) are more economical.
- *Maintenance Overheads:* Account for firmware updates, security patches, and hardware longevity.

A well-executed fog computing deployment enhances IoT system performance, security, and scalability. Organizations must carefully analyze latency demands, security protocols, network resilience, and cost factors to maximize the benefits of fog architecture. By addressing these considerations, businesses can harness fog computing's full potential – ushering in a new era of intelligent, real-time IoT ecosystems.

CONCLUSIONS

Ultimately, Fog Computing stands not merely as an architectural enhancement but as an indispensable evolutionary step for IoT. It masterfully addresses the inherent limitations of pure cloud-centric models by strategically distributing computation, storage, and networking closer to the data

origin, where time-sensitive insights are paramount. Our exploration of its layered architecture reveals a robust and flexible framework capable of delivering unprecedented low-latency responsiveness, localized data processing for enhanced privacy and regulatory compliance, and significant optimizations in bandwidth utilization, fundamentally reshaping how IoT data is processed and leveraged.

However, realizing the full promise of Fog necessitates meticulous planning for deployment, navigating persistent challenges, such as the intrinsic heterogeneity of IoT devices and Fog nodes, the complexities of dynamic resource orchestration across a vast distributed network, and the imperative for end-to-end security and interoperability across multiple vendors and protocols. The road ahead for Fog Computing involves continued innovation in areas, like intelligent resource management powered by AI, serverless Fog functions for enhanced agility, and the development of robust, standardized security protocols, that span the entire edge-to-cloud continuum. As IoT ecosystems continue their inexorable expansion, Fog will be instrumental in transforming raw data into actionable intelligence at the speed and scale required for a truly smart, autonomous, and responsive world, unlocking a new era of distributed intelligence and pervasive digital innovation.

REFERENCES

1. Mulani AO, Bang AV, Birajadar GB, Deshmukh AB, Jadhav HM, Liyakat KK. IoT based air, water, and soil monitoring system for pomegranate farming. Ann Agri-Bio Res. 2024;29(2):71–86.
2. Parihar B, Kiran A, Valaboju S, Rashid SZ, Liyakat KK, DR AS. Enhancing data security in distributed systems using homomorphic encryption and secure computation techniques. In: ITM Web Conf. 2025;76:02010. EDP Sciences.
3. Veena C, Sridevi M, Liyakat KK, Saha B, Reddy SR, Shirisha N. HEECCNB: An efficient IoT-cloud architecture for secure patient data transmission and accurate disease prediction in healthcare systems. In: 2023 7th Int Conf Image Inf Process (ICIIP). 2023. p. 407–10. IEEE.
4. Majeed R, Abdullah NA, Faheem Mushtaq M, Umer M, Nappi M. Intelligent cyber-security system for IoT-aided drones using voting classifier. Electronics. 2021;10(23):2926.
5. Chaari MZ, Al-Maadeed S. Increase the efficiency of IoT devices by using the wireless power transmission in the industrial revolution 4.0. Int J Online Biomed Eng. 2021;17(7).
6. Kanday R, Pimpale Y, Gupta S. Smart biomedical devices: smart alcohol detection system with engine cutoff and notifier. AIP Conf Proc. 2023;2800(1):020226.
7. Malek MS, Gundaliya PJ. Negative factors in implementing public–private partnership in Indian road projects. Int J Constr Manag. 2023;23(2):234–42.
8. Khatun MA, Chowdhury N, Uddin MN. Malicious nodes detection based on artificial neural network in IoT environments. In: 2019 22nd Int Conf Comput Inf Technol (ICCIT). IEEE; 2019. p. 1–6.
9. Hodo E, Bellekens X, Hamilton A, Dubouilh PL, Iorkyase E, Tachtatzis C, et al. Threat analysis of IoT networks using artificial neural network intrusion detection system. In: 2016 Int Symp Netw Comput Commun (ISNCC). IEEE; 2016. p. 1–6.
10. Lokuliyana S, Jayakody A, Dabarera GS, Ranaweera RK, Perera PG, Panangala PA. Location-based garbage management system with IoT for smart city. In: 2018 13th Int Conf Comput Sci Educ (ICCSE). IEEE; 2018. p. 1–5.
11. Sarma H, Huzuri D, Deka MK. A real-time implementation of an IoT based vehicle health monitoring system. Int J Recent Technol Eng. 2021;10:2277–3878.
12. Dinesh M, Arvind C, Sreeja Mole SS, Subash Kumar CS, Chandra Sekar P, Somasundaram K, et al. An energy efficient architecture for furnace monitor and control in foundry based on Industry 4.0 using IoT. Sci Program. 2022;2022:1128717.

