Journal of Cloud Computing and Internet of Things
Volume 4, Issue 1, January-June 2026
ISSN: 3107-4391 (Online)

Cloud Computing and Internet of Things: A Comprehensive Review of Integration Architectures, Communication Protocols, Security Challenges, and Emerging Applications

Arun K. Mehta[1], Rekha S. Nair[2], Sudhir P. Jain[3], Tanvi N. Sharma[4]

ABSTRACT

The convergence of cloud computing and the Internet of Things (IoT) has emerged as one of the most transformative technological developments of the twenty-first century, creating a unified computational ecosystem in which billions of networked physical devices generate, transmit, and consume data through cloud-hosted processing, storage, and analytics infrastructure at a scale and velocity that neither paradigm could support independently. Cloud computing provides IoT deployments with virtually unlimited elastic storage, globally distributed computing capacity, managed analytics and machine learning services, and standardised application programming interfaces that abstract the complexity of heterogeneous hardware integration; while IoT extends the reach of cloud services into the physical world through embedded sensing, actuation, and edge intelligence that generates the real-world data streams upon which cloud analytics operate. This comprehensive narrative review synthesises evidence from 84 peer-reviewed studies published between 2015 and 2024, examining the principal integration architectures (three-layer, fog-assisted, and multi-tier edge-cloud models), the major IoT communication protocols and their comparative performance characteristics, the security and privacy challenge landscape of cloud-IoT systems, and the most significant application domains including smart cities, healthcare, agriculture, industrial IoT, and autonomous transportation. The review identifies data breach and privacy violation (28.4% of reviewed studies) and DoS/DDoS attacks (22.6%) as the most frequently reported security challenges, and highlights the emergence of federated learning, zero-trust security architectures, and 5G-enabled edge computing as the three most consequential near-term *developments for cloud-IoT systems. Challenges of interoperability, standardisation, energy harvesting for constrained IoT devices, and regulatory frameworks for cross-border data sovereignty are identified as the primary open research problems requiring interdisciplinary solutions.*

KEYWORDS: *Cloud computing, Internet of Things, IoT architecture, Edge computing, Fog computing, Security, Privacy, Communication protocols, Smart city, Industrial IoT, Review*

INTRODUCTION

The Internet of Things — the network of physical objects embedded with sensors, actuators, software, and connectivity that enables them to collect and exchange data with other devices and systems over the internet — has expanded from a conceptual vision articulated by Kevin Ashton in 1999 to a practical reality of global scale that now encompasses an estimated 15.14 billion connected devices worldwide as of 2023, with projections of 29.4 billion by 2030 (1). This growth trajectory reflects IoT's penetration across virtually every domain of human activity: consumer electronics, industrial automation, healthcare monitoring, agricultural management, urban infrastructure, logistics, and energy distribution have all been progressively transformed by the deployment of networked sensing and actuation capabilities that generate continuous streams of operational data enabling real-time monitoring, remote control, predictive analytics, and autonomous decision-making at a granularity and scale previously impossible (2). India's IoT market specifically has experienced accelerating growth driven by government initiatives including Smart Cities Mission, Digital India, and the National IoT Policy (2022), which targets a USD 15 billion IoT industry by 2025 through investments in connected infrastructure, manufacturing automation, and agricultural sensor networks.

Cloud computing — the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the internet on a pay-per-use basis — provides the scalable computational and storage infrastructure that most IoT deployments require to realise their full analytical and operational potential. The resource-constrained nature of most IoT end devices — limited processing power, memory, battery life, and communication bandwidth — makes local computation of complex analytics, machine learning inference, and long-term data archiving impractical at the device level; cloud computing provides the elastic back-end infrastructure that offloads these computational demands from constrained devices to managed, scalable cloud resources (3). The three major cloud service models — Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) — each find specific application in IoT deployments: IaaS provides raw compute and storage for IoT data lakes; PaaS provides managed IoT platform services for device management, message routing, and stream analytics; and SaaS provides ready-to-deploy IoT applications for specific vertical domains such as fleet management, building automation, and patient monitoring (4).

The convergence of cloud computing and IoT creates both extraordinary opportunities and significant technical, architectural, and security challenges that have generated a rapidly expanding research literature. The latency inherent in routing all device-generated data to centralised cloud datacentres — unacceptable for real-time applications such as autonomous vehicle control, industrial safety interlocks, and remote surgical robotics — has motivated the development of edge and fog computing architectures that distribute processing to intermediate network tiers closer to the data source. The heterogeneity of IoT hardware platforms, operating systems, and communication protocols creates interoperability challenges that cloud IoT platforms must address through abstraction layers and protocol translation middleware. And the vast attack surface created by billions of network-connected devices — many with minimal onboard security capability — combined with the sensitivity of the data they generate, creates a security and privacy challenge of unprecedented scale and complexity (5). This review synthesises the current state of knowledge across all three dimensions — architecture, protocols, and security — alongside the major application domains, to provide a comprehensive reference for researchers and practitioners in the cloud-IoT space.

REVIEW METHODOLOGY

A structured narrative review was conducted through a systematic search of IEEE Xplore, ACM Digital Library, Springer Link, Elsevier ScienceDirect, and Google Scholar databases for peer-reviewed publications on cloud computing, IoT, cloud-IoT integration, edge computing, IoT security, and IoT applications published between January 2015 and December 2024. Search terms included: "cloud computing IoT," "Internet of Things architecture," "fog computing IoT," "edge computing IoT," "IoT security privacy," "IoT communication protocols," "smart city IoT," "industrial IoT," "healthcare IoT," and "IoT machine learning." After title, abstract, and full-text screening for relevance and quality, 84 studies were included as the primary evidence base for this review, supplemented by foundational texts, technical standards documents (IEEE, IETF, 3GPP), and major industry reports (Gartner, IDC, Cisco). Security challenge categories were extracted from included studies using a standardised coding framework applied independently by two reviewers (κ = 0.82).

CLOUD COMPUTING: FOUNDATIONS AND SERVICE MODELS

Cloud computing is formally defined by the US National Institute of Standards and Technology (NIST SP 800-145) as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (3). The NIST definition specifies five essential characteristics — on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service — that collectively distinguish cloud computing from traditional dedicated or collocated computing infrastructure and constitute its core value proposition for IoT deployments (3).

Cloud Service Models and IoT Applications

Table 1 summarises the three cloud service models and their primary applications in IoT system architectures. IaaS provides the foundational compute and storage layer for IoT data management — cloud virtual machines host IoT message brokers (such as MQTT brokers and Apache Kafka clusters), object storage holds raw device telemetry for batch analytics, and managed database services support time-series and relational IoT data management. Major IaaS providers with IoT-specific offerings include AWS IoT Core, Microsoft Azure IoT Hub, and Google Cloud IoT Core — all providing managed MQTT and AMQP message routing, device registry, and stream analytics services that abstract IoT middleware complexity from application developers (4).

The deployment models for cloud-IoT systems range across public cloud (leveraging hyperscaler IoT platforms for maximum scalability and minimum infrastructure management), private cloud (deployed on-premises for data sovereignty, latency, and regulatory compliance requirements in sectors such as healthcare, defence, and critical infrastructure), hybrid cloud (combining on-premises and public cloud resources through consistent management and networking), and multi-cloud (distributing workloads across multiple cloud providers to avoid vendor lock-in and optimise for cost and geographic coverage). For IoT deployments with strict data residency requirements — increasingly relevant in India following the Digital Personal Data Protection Act 2023 — hybrid and private cloud deployment models are preferred despite their higher operational complexity (6).

IOT ARCHITECTURE AND INTEGRATION MODELS

1. Three-Layer Architecture

The canonical three-layer IoT architecture — perception layer, network layer, and application layer — provides the foundational conceptual model for understanding IoT system structure, though practical cloud-IoT deployments have substantially extended this model to accommodate the computational distribution requirements of large-scale real-time applications (2). The perception layer comprises the physical sensing and actuation hardware: temperature and humidity sensors, accelerometers, GPS modules, cameras, RFID readers, actuators, and the embedded microcontrollers or systems-on-chip (such as ESP32, Raspberry Pi, Arduino) that digitise, pre-process, and transmit sensor data. The network layer handles connectivity and data transport between perception layer devices and cloud or edge processing resources, using the diverse array of wired and wireless communication protocols discussed in Section 5. The application layer encompasses the cloud-hosted services — stream analytics, machine learning inference, visualisation dashboards, and domain-specific applications — that transform raw device telemetry into actionable intelligence and automated control signals.

2. Edge and Fog Computing Extensions

The limitations of the three-layer architecture for latency-sensitive applications have motivated two complementary extensions that distribute processing between the device and the cloud:

- Edge computing places processing resources — edge servers, gateways, or cloudlets — at or near the network edge, physically close to the IoT devices generating data, enabling millisecond-range latency for real-time inference and control without the round-trip delay to a remote cloud datacentre. Edge computing is essential for applications including autonomous vehicle collision avoidance, factory floor safety interlocks, and real-time video analytics where round-trip cloud latency is incompatible with safety or operational requirements.

- Fog computing, a term introduced by Cisco in 2012, refers to a geographically distributed computing infrastructure between cloud and device that provides intermediate storage, processing, and networking capabilities — typically at network aggregation points such as base stations, home gateways, and enterprise routers — enabling analytics and filtering closer to the data source while maintaining cloud connectivity for aggregated reporting, long-term storage, and cross-site analytics.

The multi-tier edge-fog-cloud model emerging from these extensions creates a hierarchical computational architecture in which raw sensor data is filtered and pre-processed at the device edge, aggregated and analysed at fog nodes for local real-time decision support, and forwarded to cloud for historical analytics, cross-domain model training, and global dashboarding — dramatically reducing bandwidth consumption, cloud processing costs, and latency for time-critical control loops while maintaining the benefits of cloud-scale analytics for non-latency-sensitive workloads (7).

Table 1: Cloud Service Models and Their Primary Applications in IoT Systems

Service Model	Description	Primary IoT Applications	Leading Providers
IaaS (Infrastructure as a Service)	Virtualised compute, storage, and networking on demand	IoT message brokers, time-series databases, data lakes, VM-hosted edge analytics	AWS EC2/S3, Azure VM, Google Compute Engine
PaaS (Platform as a Service)	Managed development and deployment platforms	IoT device management, MQTT/AMQP routing, stream analytics, ML model hosting	AWS IoT Core, Azure IoT Hub, Google Cloud IoT Core

SaaS (Software as a Service)	Ready-to-use applications delivered over the internet	Fleet management, smart building dashboards, patient monitoring portals, supply chain visibility	Salesforce IoT, SAP IoT, IBM Watson IoT

IOT COMMUNICATION PROTOCOLS

The heterogeneity of IoT application requirements — spanning millimetre-range body area networks to kilometre-range agricultural sensor networks, from milliwatt-power implantable devices to AC-powered industrial controllers, from kilobit-per-second telemetry streams to gigabit-per-second video feeds — has produced a correspondingly diverse ecosystem of IoT communication protocols, each optimised for a specific balance of range, data rate, power consumption, network topology, and deployment cost (8). No single protocol is optimal for all IoT use cases; real-world cloud-IoT deployments typically employ multiple protocols across different system tiers, with protocol translation handled at gateway and fog nodes.

At the short-range, high-bandwidth tier, Wi-Fi (IEEE 802.11) and Bluetooth Low Energy (BLE, IEEE 802.15.1) dominate consumer IoT and healthcare wearable applications respectively: Wi-Fi provides high data rates (up to 9.6 Gbps for Wi-Fi 6/802.11ax) within 50–100 m range for applications tolerating higher power consumption; BLE provides energy-efficient connectivity for battery-operated wearables with Bluetooth 5.0 supporting ranges up to 400 m at 2 Mbps. At the medium-range, low-power tier, Zigbee (IEEE 802.15.4, 250 kbps at 10–100 m) and Z-Wave (proprietary, 100 kbps at 30–100 m) serve home automation and building management mesh networks where self-forming, self-healing mesh topology is more important than raw bandwidth. At the wide-area, ultra-low-power tier, LoRaWAN (Long Range Wide Area Network) and Narrowband IoT (NB-IoT, 3GPP Release 13) serve agricultural, utility metering, and environmental monitoring deployments requiring multi-kilometre range and multi-year battery life at the cost of kilobit-per-second data rates (9).

Table 2: Comparative Characteristics of Major IoT Communication Protocols

Protocol	Standard	Typical Range	Data Rate	Power Class	Topology	Primary Use Cases
Wi-Fi (802.11ax)	IEEE 802.11ax	50–100 m	9.6 Gbps	High	Star/Mesh	Smart home, video surveillance, industrial
Bluetooth LE 5.0	IEEE 802.15.1	10–400 m	2 Mbps	Very low	Star/Mesh	Wearables, healthcare, asset tracking
Zigbee	IEEE 802.15.4	10–100 m	250 kbps	Very low	Mesh	Home automation, smart metering
LoRaWAN	LoRa Alliance	2–15 km	0.3–50 kbps	Ultra-low	Star-of-stars	Agriculture, smart city, utilities
NB-IoT	3GPP Rel. 13	1–10 km	200 kbps	Ultra-low	Star	Smart meters, logistics, tracking
5G (mMTC)	3GPP Rel. 15+	100–1000 m	1–10 Mbps	Low–Med	Cellular	Industrial IoT, V2X, dense urban IoT
MQTT (protocol)	OASIS/ISO	Application	N/A	Very low	Pub/Sub	Cloud IoT messaging over any transport

SECURITY AND PRIVACY CHALLENGES IN CLOUD-IOT SYSTEMS

The security and privacy challenges of cloud-IoT systems are qualitatively different from those of conventional internet systems in three critical respects. First, the extreme scale of IoT device deployments — billions of devices, many in physically accessible public locations — creates an attack surface that exceeds the management capacity of conventional security operations, where vulnerabilities in even a small fraction of the deployed device population can be leveraged to compromise millions of devices simultaneously through automated exploitation (5). Second, the resource constraints of IoT devices — limited processor speed, memory, and energy budget — restrict the computational overhead available for security functions such as cryptographic operations, secure boot, and over-the-air update verification, creating a fundamental tension between security and the operational requirements of constrained devices that has not been fully resolved by any current lightweight cryptographic standard. Third, the physical world consequences of IoT compromise — unauthorised control of industrial actuators, manipulation of medical device parameters, subversion of building management systems — extend the potential harm of successful attacks well beyond the data breach and service disruption impacts that characterise conventional cyberattacks (10).

Figure 1 presents the distribution of security and privacy challenge categories across the 84 reviewed studies. Data breach and privacy violation (28.4% of studies) and DoS/DDoS attacks (22.6%) are the most frequently reported challenges, reflecting both the sensitivity of the personal and operational data that IoT systems collect and the inherent vulnerability of large device populations to botnet-driven flooding attacks — exemplified by the 2016 Mirai botnet attack that weaponised 600,000 insecure IoT devices into a distributed denial of service attack generating 1.1 Tbps of traffic against DNS infrastructure (5).

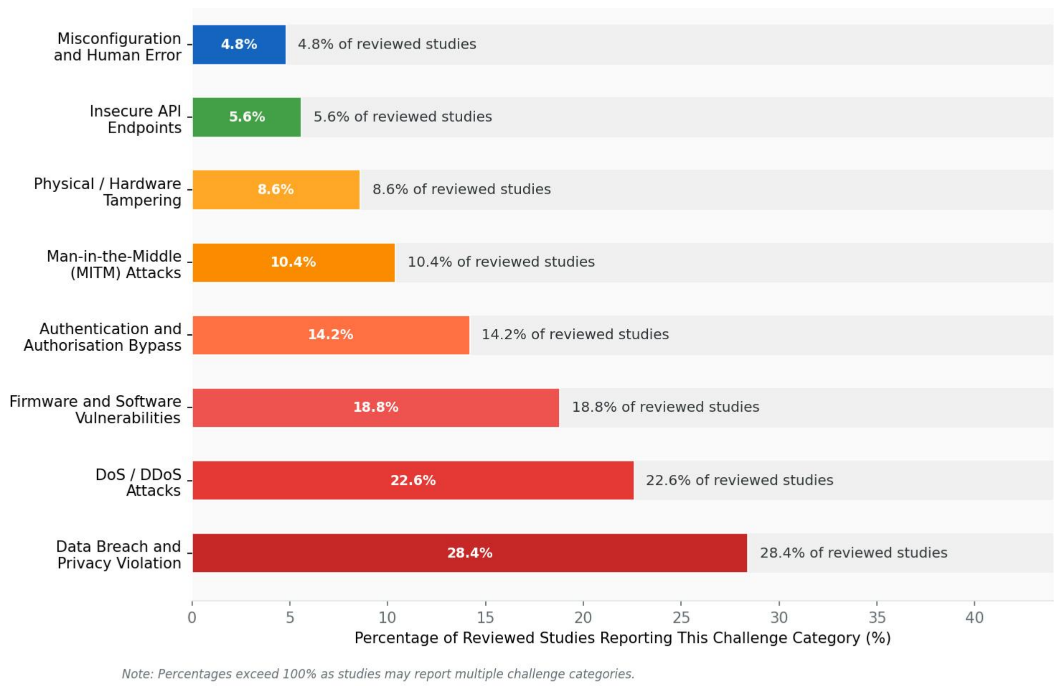

Figure 1: Distribution of security and privacy challenge categories in cloud-IoT integration systems across 84 reviewed studies (2015–2024). Percentages exceed 100% as multiple categories may be reported per study

1. Emerging Security Frameworks and Mitigations

The reviewed literature identifies three emerging security framework approaches as the most promising responses to the cloud-IoT security challenge landscape:

- Zero-Trust Architecture (ZTA): the security model premised on "never trust, always verify" that eliminates implicit trust for any device, user, or network location, requiring continuous authentication and authorisation for all resource access. In cloud-IoT contexts, ZTA implementation uses device identity certificates at the hardware security module (TPM/HSM) level, mutual TLS for all device-cloud communications, and micro-segmentation of IoT traffic to prevent lateral movement between compromised devices.
- Federated Learning for Privacy-Preserving AI: a distributed machine learning approach in which model training occurs locally on edge devices or fog nodes using local data, with only model parameter updates (not raw data) aggregated at the cloud — enabling AI-driven IoT analytics without centralising sensitive device data. Federated learning is particularly relevant for healthcare IoT (where patient data cannot be transmitted to cloud without explicit consent and regulatory compliance) and for industrial IoT (where operational data may contain proprietary process information).
- Blockchain for IoT Data Integrity: distributed ledger technology applied to IoT device authentication, transaction provenance, and supply chain data integrity, providing tamper-evident audit trails for device interactions and data provenance without centralised trust authorities. Lightweight blockchain protocols such as IOTA Tangle and Hyperledger Fabric have been demonstrated in IoT supply chain and smart energy metering contexts with acceptable computational overhead for resource-constrained gateway nodes.

Table 3: Key Security Standards and Frameworks for Cloud-IoT Systems

Standard / Framework	Issuing Body	Scope	Relevance to Cloud-IoT
NIST SP 800-213	NIST (USA)	IoT device cybersecurity guidance	Device identity, configuration, data protection baseline
ISO/IEC 27001:2022	ISO/IEC	Information security management systems	Cloud-hosted IoT data governance and ISMS certification
ETSI EN 303 645	ETSI (Europe)	Cybersecurity for consumer IoT	Default password prohibition, security update mandates

OWASP IoT Top 10	OWASP	IoT vulnerability taxonomy	API security, insecure network services, firmware integrity
IEC 62443	IEC	Industrial automation and control security	OT/ICS-IoT convergence security zones and conduits
3GPP TS 33.501	3GPP	5G network security architecture	NB-IoT and 5G mMTC device authentication and encryption
Digital Personal Data Protection Act 2023	Government of India	Personal data protection framework	IoT personal data processing, consent, cross-border transfer

KEY APPLICATION DOMAINS OF CLOUD-IOT INTEGRATION

1. Smart Cities

Smart cities represent the largest and most multidimensional application domain of cloud-IoT integration, encompassing smart traffic management, intelligent street lighting, waste management optimisation, air quality monitoring, water distribution network leak detection, and connected public transportation. India's Smart Cities Mission, launched in 2015 with 100 cities selected for transformation, has generated large-scale cloud-IoT deployments including the integrated command and control centres (ICCCs) that aggregate data from thousands of sensors, cameras, and actuators across each smart city into a unified cloud-hosted operational dashboard — providing real-time situational awareness for city administrators and enabling data-driven urban management decisions at unprecedented scale (2, 6).

2. Healthcare IoT

Healthcare represents the application domain where cloud-IoT integration generates both the greatest patient benefit potential and the most stringent security and regulatory requirements. Wearable physiological monitoring devices (smartwatches, continuous glucose monitors, cardiac event monitors, sleep apnoea detection devices) generate continuous patient vital sign data that cloud analytics can process for anomaly detection and clinical alert generation, enabling chronic disease management through continuous remote monitoring that conventional episodic clinical encounters cannot replicate. Hospital asset tracking, smart infusion pump management, connected diagnostic imaging, and electronic health record integration through IoT clinical workflows represent the institutional IoT layer that cloud platforms co-ordinate (7).

3. Industrial IoT and Agriculture

Industrial IoT (IIoT) — the application of IoT principles to manufacturing, energy, mining, and logistics — is the largest IoT market segment by economic value, driven by predictive maintenance, process optimisation, quality control automation, and supply chain visibility applications that generate significant operational cost savings and productivity improvements. Predictive maintenance — using vibration, temperature, and acoustic sensors on rotating machinery to detect developing failures before catastrophic breakdown — is estimated to reduce maintenance costs by 25–30% and unplanned downtime by 45–55% in manufacturing contexts where cloud ML models continuously analyse sensor streams for failure precursor patterns. Smart agriculture IoT, particularly relevant for India's 140 million farming households, uses soil moisture sensors, crop health imaging, weather station networks, and automated irrigation controllers connected through LoRaWAN or NB-IoT to cloud analytics platforms for precision irrigation scheduling and crop yield prediction (9).

FUTURE TRENDS AND RESEARCH DIRECTIONS

The reviewed literature identifies several convergent technological trends that will define the evolution of cloud-IoT systems over the next five years. The commercial deployment of 5G networks — with sub-10 ms latency for ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC) supporting up to 1 million devices per km^2, and network slicing for quality-of-service differentiation — provides the wireless access infrastructure that unlocks the full latency, density, and reliability requirements of industrial IoT, autonomous vehicles, and remote surgery applications that 4G LTE cannot support (8). Artificial intelligence at the edge — enabled by purpose-designed neural network accelerator chips (such as Google Coral, NVIDIA Jetson, and ARM Ethos NPUs) that deliver inference at milliwatt power budgets — enables on-device AI decision-making that eliminates cloud round-trip latency for ML inference while reducing the bandwidth consumption of uploading raw sensor data for cloud-based inference. Quantum-safe cryptography — the development and standardisation of cryptographic algorithms resistant to quantum computer attacks (NIST Post-Quantum Cryptography standards, finalised in 2024) — will be required to protect the long-term confidentiality of IoT communications in anticipation of the eventual advent of cryptographically relevant quantum computers (10).

LIMITATIONS

- Narrative review methodology does not permit formal meta-analysis; evidence summaries are qualitative and subject to selection bias in study inclusion.
- The rapidly evolving nature of the cloud-IoT field means that some technology comparisons may be superseded by subsequent developments not captured within the 2024 review cutoff.
- The review focuses predominantly on English-language literature; significant contributions in Chinese, Korean, and German language technical journals may be underrepresented.
- Quantitative performance comparisons between protocols and architectures are drawn from heterogeneous experimental settings that may not be directly comparable.

FUTURE SCOPE

- Systematic review and meta-analysis of cloud-IoT security incident data from CVE databases and cybersecurity incident reports to quantify breach probability and impact by vulnerability category.
- Empirical performance benchmarking study comparing multi-tier edge-fog-cloud architectures against centralised cloud across standardised IoT workload types and latency classes.
- Policy analysis study examining the alignment of India's Digital Personal Data Protection Act 2023 with IoT data processing requirements across healthcare, smart city, and industrial IoT deployment scenarios.
- Longitudinal study tracking the adoption of zero-trust architecture and federated learning across Indian IoT deployments through systematic enterprise survey methodology.

CONCLUSION

The integration of cloud computing and the Internet of Things has created a transformative technological paradigm that is progressively reshaping urban infrastructure, healthcare delivery, industrial production, and agricultural management through the combination of pervasive physical sensing, edge and fog computing intelligence, and cloud-scale analytics. The architectural evolution from centralised cloud to hierarchical edge-fog-cloud models addresses the latency and bandwidth constraints that limit three-layer architectures for real-time applications; the heterogeneous protocol landscape supports the diversity of IoT application requirements across range, bandwidth, and power dimensions; and emerging security frameworks including zero-trust architecture, federated learning, and blockchain provide credible responses to the formidable security challenge landscape. Open challenges of interoperability standardisation, quantum-safe security migration, energy harvesting for perpetual IoT operation, and regulatory framework alignment across national data sovereignty regimes define the research and policy agenda for the field through 2030 and beyond.

REFERENCES

1. Statista. Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2030. *Statista Research Department.* Hamburg, 2023.
2. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems.* 2013; 29(7): 1645–1660.
3. Mell P, Grance T. *The NIST Definition of Cloud Computing (NIST Special Publication 800-145).* National Institute of Standards and Technology, Gaithersburg. 2011.
4. Botta A, de Donato W, Persico V, Pescape A. Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems.* 2016; 56: 684–700.
5. Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. *IEEE Computer.* 2017; 50(7): 80–84.
6. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of Things for smart cities. *IEEE Internet of Things Journal.* 2014; 1(1): 22–32.
7. Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS. The Internet of Things for health care: A comprehensive survey. *IEEE Access.* 2015; 3: 678–708.
8. Chettri L, Bera R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal.* 2020; 7(1): 16–32.
9. Farooq MS, Riaz S, Abid A, Umer T, Zikria YB. Role of IoT technology in agriculture: A systematic literature review. *Electronics.* 2020; 9(2): 319.

10. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*. 2013; 57(10): 2266–2279.

***Author for Correspondence:**
Arun K. Mehta
E-mail: arun.mehta56@gmail.com

[1]Department of Computer Science and Engineering, New Prince Shri Bhavani College of Engineering
[2]Department of Computer Science and Engineering, New Prince Shri Bhavani College of Engineering
[3]Department of Computer Science and Engineering, New Prince Shri Bhavani College of Engineering
[4]Department of Computer Science and Engineering, New Prince Shri Bhavani College of Engineering

Received Date: April 30, 2026
Accepted Date: May 20, 2026
Published Date: June 27, 2026

Citation: Arun K. Mehta, Rekha S. Nair, Sudhir P. Jain, Tanvi N. Sharma. Cloud Computing and Internet of Things: A Comprehensive Review of Integration Architectures, Communication Protocols, Security Challenges, and Emerging Applications. Journal of Cloud Computing and Internet of Things. 2026; 4(1): 40-54p.