International Journal of Current Engineering and Technology
E-ISSN 2277-4106, P-ISSN 2347-5161

Available at https://ijcet.evegenis.org/index.php/ijcet/index

Review Article

Generative Artificial Intelligence for Smart IoT Systems: A Comprehensive Review

Bal Krishna Sharma*

Professor Department of Computer Science and Application, Mandsaur University, Mandsaur (MP), India

Received 01 Sep 2026, Accepted 22 Sep 2026, Available online 24 Sep 2026, **Vol.16, No.5 (Sep/Oct 2026)**

Abstract

The Internet of Things (IoT) has transformed conventional devices and environments into interconnected smart systems capable of sensing, communicating, and processing real-time data. However, the increasing scale, heterogeneity, resource constraints, security concerns, and massive volume of IoT-generated data create significant challenges for intelligent decision-making and autonomous operation. Generative Artificial Intelligence (GenAI) provides emerging capabilities for generating synthetic data, interpreting complex information, supporting prediction, enabling personalization, and facilitating human-machine interaction. This review presents a comprehensive analysis of Generative AI for Smart IoT Systems, covering IoT networking technologies, data-driven approaches, architectures, components, applications, and existing challenges. It further examines GenAI-enabled IoT architectures, including edge-cloud, federated, and autonomous approaches, as well as opportunities in model compression, runtime optimization, and edge-cloud collaboration. Applications in smart homes, healthcare, industrial IoT, smart cities, mobile networks, cybersecurity, and digital twins are discussed. Recent studies are comparatively analyzed to identify key findings, limitations, and research directions. Finally, the review highlights emerging opportunities and challenges for developing secure, scalable, efficient, adaptive, and intelligent GenAI-driven IoT ecosystems.

Keywords: *Generative Artificial Intelligence, Smart Internet of Things, Edge Computing, IoT Systems, Intelligent Automation*

Introduction

The applications of smart devices are becoming increasingly widespread in daily life, with modern technologies incorporating Internet of Things (IoT) components to provide enhanced intelligence and functionality [1]. IoT enables interconnected devices, sensors, and systems to collect, communicate, and process data across diverse environments and applications [2]. IoT-based devices are widely deployed in areas such as healthcare, where wearable sensors can continuously monitor parameters including blood pressure, body temperature, and heart-related conditions. These sensors collect and transmit data through communication technologies for further processing and decision-making [3]. The IoT has therefore evolved into a network of interconnected devices that enables interactions between objects, systems, and users anytime and anywhere, creating significant opportunities for intelligent applications and services [4].

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: DOI: https://doi.org/10.14741/ijcet/v.16.5.1

Generative Artificial Intelligence (GenAI) has emerged as a transformative paradigm that extends the capabilities of traditional AI through advanced deep generative models. Its ability to generate synthetic data, handle uncertainty, interpret complex information, and produce human-like content provides new opportunities for addressing challenges in IoT systems. In particular, GenAI can support data generation, processing, interpretation, prediction, optimization, autonomous decision-making, and real-time human–machine interaction [5]. These capabilities are particularly relevant to smart IoT environments because of their dynamic, distributed, heterogeneous, and resource-constrained nature. GenAI can help improve data quality, system reliability, predictive capabilities, and intelligent decision-making while enabling realistic scenario generation and adaptive IoT operations [6]. Therefore, integrating GenAI with smart IoT systems represents an emerging research direction with significant potential, although its implementation also introduces new technical and practical challenges that require systematic investigation. This paper is divided into five sections: Section II introduces Smart IoT Systems. Section III explores Generative Artificial Intelligence for Smart IoT Systems. Section IV reviews recent literature, and Section V concludes the paper while outlining potential future research directions.

Smart IoT Systems Architecture and Technologies

The phrase "Internet of Things", which is also commonly known as IoT, is coined from the two words, i.e., the first word is "Internet" and the second word is "Things" [7]. The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks comprising millions of private, public, academic, business, and government networks, ranging in scope from local to global, linked by a broad array of electronic, wireless, and optical networking technologies.

IoT Networking Technologies

In this section, different IoT connectivity technologies, cellular requirements and standards for the IoT are discussed elaborately.

In this section, different IoT connectivity technologies, cellular requirements, and standards for the IoT are discussed elaborately [8].

Connectivity Technologies: Connectivity solutions for the IoTs are crucial for facilitating communication between systems and objects that make up the IoT. These technologies vary in range, bandwidth, power consumption, and suitability for application. There are several IoT technologies available for connectivity, each with its own set of advantages and use cases.

3GPP Cellular MTC: Within the cellular context, the IoT connectivity solution is referred to as Machine-to-Machine (M2M), and within the 3GPP standardization body, it is referred to as Machine-Type Communications (MTC) [9].

MTC Requirements and Standards: MTC (Machine-Type Communication) refers to communication between machines or devices in the context of the IoT.

3GPP MTC Standardization: 3GPP (Third Generation Partnership Project) is a global standardization organization that develops specifications for mobile communication systems, including MTC (Machine-Type Communication) in the context of the IoT.

Data-Driven Approach to IoT

The data-driven approach to IoT leverages the vast amount of data generated by interconnected devices to derive actionable insights, optimize system performance, and enhance user experiences [10]. By integrating advanced data analytics and ML techniques, this approach enables intelligent decision-making and automation.

Data Collection and Preprocessing: Data collection is the foundational step in the data-driven approach to IoT, where raw data is gathered from various sensors embedded in devices, machines, and environments. These sensors capture a wide range of data, including temperature, humidity, motion, light intensity, and more.

Data Storage and Management: Efficient data storage and management are critical for IoT systems due to the sheer volume, velocity, and variety of data generated by interconnected devices [11]. Conventional relational databases that depend on rigid schemas and structured data models could be inappropriate for handling dynamic and unstructured data produced by the IoT.

Data Analytics and Machine Learning: Data analytics and ML are the heart and soul of the data-driven methodology of the IoT as they make raw data into something meaningful and help people make decisions. The process of data analytics uses computational methods to discover patterns, connections, and trends in the data.

Architecture of Smart IoT Systems

There is no established standard or technology used in IoT devices and platforms at the moment. Different devices and platforms use different standards and technologies [12]. Therefore, deploying an IoT system often requires users to study, configure, and integrate various architectures and technologies, which can make the process difficult and time-consuming. Fig. 1. IoT architecture illustrates the layered IoT architecture comprising sensors and actuators, communication networks, IoT gateways, platforms, applications, security, and management for integrated service delivery.

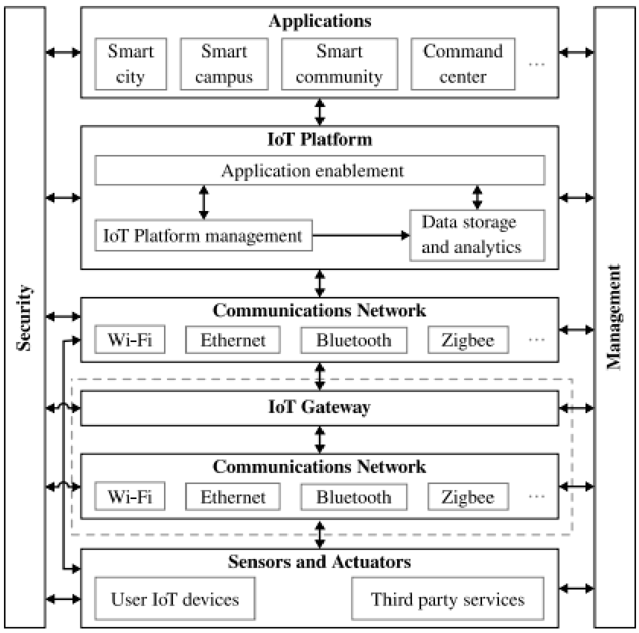


Fig.1 IoT Architecture

Sensors and actuators: Sensors are hardware devices that measure physical parameters from the environment or from other systems. Actuators are hardware devices that carry out actions based on IoT requests. Usually, these are small devices with limited resources, and in the simplest cases the needed processing capabilities may be achieved using a small microcontroller without an operating system [13].

Communications network: To enable data exchange among sensors, actuators, and the IoT platform and gateway components one or more communications networks must be in place. The communications network must provide the physical, link, and network layers according to the Open Systems Interconnection (OSI) model.

IoT gateway: Different IoT devices may use different communication networks, data layer protocols and, in many cases, the IoT platform may lack direct support for some of these. To solve this problem, a middleware component called a " gateway " or ‘‘edge gateway’’ may be introduced between the IoT platform and the IoT devices. The gateway provides a common communication network, a data-layer protocol, and a data format for communication with the IoT platform. In real scenarios, several gateway devices may be deployed, with each gateway connecting to several IoT devices.

IoT platform: The IoT platform is the central hub of the IoT system, enabling the connected sensors and actuators to be controlled and monitored with the help of applications. It consists of three fundamental building blocks: device management and connectivity, data storage and analytics, and application enablement.

Applications: An application is a software component that performs a specific task, reading data captured by the sensors and/or controlling the actuators. Examples of applications include a GUI graph that displays sensor data over time. A GUI button that allows the user to turn on or off some device. A rule that automatically turns on or off a device based on the values provided by another sensor.

Components of Smart IoT Systems

IoT technology involves a complex structure where numerous devices and systems connect to collect, transmit, and process data. The four main layers (Fig.2) that enable the operation of IoT complement each other and perform distinct functions to ensure the system operates smoothly. A smart IoT system integrates interconnected layers that collectively support sensing, communication, data processing, and user-oriented services. These parts allow Internet of Things devices to sense their actual surroundings, send and process that data, and then use that analysis to provide useful results in a variety of contexts [14]. The major components are shown in Figure 2 below:

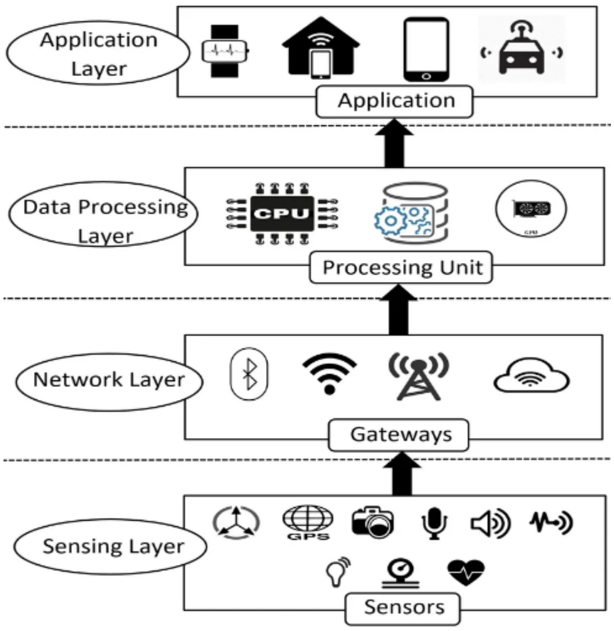


Fig.2 IoT Architecture Layers and Components[15]

Application Layer: The application layer implements and presents the results of the data processing layer to accomplish disparate applications of IoT devices. The application layer is a user-centric layer that executes various tasks for the users. There are diverse IoT applications, including smart transportation, smart homes, personal care, healthcare, etc.

Data Processing Layer: The data processing layer consists of the main data processing unit of IoT devices. The data processing layer takes data collected in the sensing layer and analyses the data to make decisions based on the result. In some IoT devices (e.g., smartwatches, smart home hubs), the data processing layer also saves the results of previous analyses to improve the user experience. This layer may share the results of data processing with other connected devices via the network layer.

Network Layer: The network layer acts as a communication channel to transfer data, collected in the sensing layer to other connected devices. In IoT devices, the network layer is implemented using diverse communication technologies (e.g., Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, cellular networks) to enable data exchange between devices within the same network.

Sensing Layer: The main purpose of the sensing layer is to identify any phenomena in the devices' peripherals and obtain data from the real world. This layer consists of several sensors. Using multiple sensors in applications is a primary feature of IoT devices. Sensors in IoT devices are usually integrated through sensor hubs. A sensor hub is a common connection point for multiple sensors, aggregating and forwarding their data to a device's processing unit. A sensor hub uses several transport mechanisms (Inter-Integrated Circuit (I2C) or Serial Peripheral Interface (SPI)) for data to go between sensors and applications.

These transport mechanisms rely on IoT devices and establish a communication channel between sensors and applications for data collection.

Application of Smart IoT Systems

The vast potential of the IoTs is being explored in diverse fields [16]. New applications are being developed which are making a difference to people's everyday lives and impacting the environments in which live, work, travel, exercise.

Smart Home: A smart home consists of advanced automation systems that handle various tasks such as overseeing and managing household appliances, multimedia equipment, security systems [17], as well as controlling lighting and temperature settings from a remote location. The aim of this system is to raise living standards, security and safety while conserving resources and energy.

Smart Parking: IoT is addressing traffic congestion, limited parking, and street security. To mitigate these issues, various parking management systems have been established to reduce traffic problems and enhance car usage convenience[18]. A smart parking system is created by combining smartphones, wireless algorithms, and mobile applications.

Smart Traffic: The IoTs is a technology that utilizes sensors and cloud-based algorithms to monitor and manage traffic. In this process, traffic cameras play an essential role, along with other technologies, such as using Wi-Fi, Bluetooth, and Zigbee signals from smart devices in cars to analyze traffic patterns.

Challenges of Smart IoT Systems

Testing IoT systems introduces challenges stemming from heterogeneity, scale, and resource constraints [19]. Addressing them requires rethinking conventional software testing strategies and adopting specialized tools, new methodologies, and interdisciplinary approaches.

Heterogeneity of Hardware and Software: IoT environments consist of a wide variety of hardware devices, including microcontrollers, embedded sensors, actuators, gateways, and network routers [20]. These components often come from different manufacturers, use different instruction sets and operate on distinct operating systems and firmware stacks.

Unstable Connectivity and Protocol Diversity: IoT systems operate over a wide range of network conditions, from high-speed Wi-Fi to low-bandwidth, lossy networks such as LoRaWAN or ZigBee [21]. Furthermore, IoT communication often involves lightweight protocols, such as MQTT, CoAP, and 6LoWPAN, which are optimized for constrained environments but introduce unique behaviours, such as publish/subscribe models and unreliable transport layers.

Scalability and Data Volume: Many IoT deployments involve hundreds or thousands of devices transmitting data simultaneously. Managing the orchestration, coordination, and testing of such a large number of endpoints introduces both technical and logistical complexities.

Resource Constraints on Devices: IoT devices often have severe limitations in terms of memory, CPU, storage, and battery life [22]. These constraints impact not only the design of the system but also the testing process itself.

Generative Artificial Intelligence for Smart IoT Systems

The Internet of Things generates enormous quantities of real-time data from connected devices, ranging from smart thermostats and wearable health monitors to industrial machinery [23]. The data explosion requires immediate data analysis to obtain actionable insights and make decisions. Traditional methods of data analysis lack the required speed and scale to analyze the complexity and huge amounts of data that IoT generates. Generative AI tackles this problem by providing powerful means for automated data analysis. Generative AI can detect patterns in IoT sensors' data that may indicate equipment malfunction.

Architecture Of Generative AI-Enabled IoT Systems

In IoT systems, acquiring diverse and high-quality datasets is often constrained by data sparsity, privacy regulations, and the difficulty of capturing rare or sensitive events, such as cyberattacks [24]. Generative AI models, including LLMs and multimodal systems, provide an innovative solution to this challenge, as illustrated in Figure 3. which describes the architecture of Generative AI.

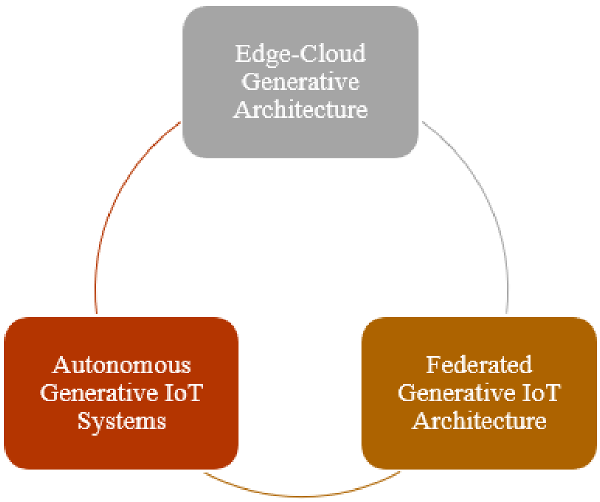


Fig.3 Generative AI-Enabled IoT System Architecture

Edge-Cloud Generative Architecture: In this model, lightweight generative inference runs on edge devices while training occurs in cloud servers [25]. IoT Devices: Sensors and actuators collect data, Edge

Nodes: Local inference and preprocessing, Cloud AI: Model training and updates, Application Services: Decision and automation [26].

Federated Generative IoT Architecture: Federated learning allows multiple IoT devices to collaboratively train generative models without sharing raw data.

Autonomous Generative IoT Systems: Future IoT systems may use self-learning generative agents embedded in devices capable of local reasoning and adaptation. Such systems continuously learn environment patterns and generate optimal actions [27].

IoT Integration for Smart Environments

The integration of the Internet of Things (IoT) within smart environments serves as a fundamental enabler for autonomous and intelligent operations. In the context of the proposed Intelligent Autonomous Robotics System (IARS), IoT acts as the connective framework that bridges the physical world with the digital intelligence layer. Through a network of distributed sensors, actuators and communication modules, IoT enables continuous monitoring, data collection and control of environmental parameters across diverse domains such as urban infrastructure, waste management and industrial automation. IoT devices within smart environments are designed to capture real-time data on temperature, air quality, humidity, waste levels, and energy consumption. These devices utilize standardized communication protocols such as MQTT, CoAP, and HTTP/REST to ensure interoperability across heterogeneous platforms. Smart environments that incorporate the IoT are crucial to the development of autonomous and intelligent operations. Specifically, the IoT serves as the backbone that links the real world to the digital intelligence layer inside the IARS proposal [28]. Through a network of distributed sensors, actuators, and communication modules, IoT enables continuous monitoring, data collection, and control of environmental parameters across diverse domains such as urban infrastructure, waste management and industrial automation. IoT devices within smart environments are designed to capture real-time data on temperature, air quality, humidity, waste levels, and energy consumption. These devices utilize standardized communication protocols such as MQTT, CoAP, and HTTP/REST to ensure interoperability across heterogeneous platforms.

Opportunities of Enabling Generative AI for IoT

There are many opportunities for enabling generative AI for IoT few opportunities are listed below:

Build Generative Models for IoT Data: The lack of generative models for IoT data hinders the development of generative AI-assisted IoT applications [29]. Therefore, there is a significant opportunity for researchers and practitioners to develop new generative models to analyze or generate various IoT data.

Model Compression: Model deployment and content production on IoT devices can be challenging due to limited memory and computing resources. One useful solution is to compress the generative models14 before distribution.

Optimization at Runtime: Model compression reduces the memory and compute resource demands of generative models before they are deployed on IoT devices [30].

Edge-Cloud Collaboration: Given the limited memory and compute resources, some IoT devices may not be able to even run the models that are already compressed.

Applications of Generative Ai in Iot

There are so many applications of Generative AI in IoT, some of them are mentioned below:

Mobile Networks: Generative AI has found its use cases in the design and operation of mobile networks [31]. For instance, understanding channel distribution is essential to comprehending the sophisticated dynamics of mobile networks.

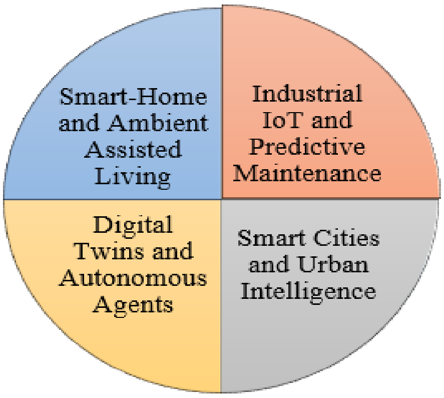
Metaverse: The role of IoT devices in a Metaverse construction is to collect live stream data, which builds a channel between real-world objects and virtual entities, enabling synchronized interactions.

Health Care: The healthcare sector, empowered by IoT devices, is experiencing a transformative paradigm shift with the integration of Generative AI. These advancements not only enable devices to monitor patient vitals but also predict and generate responses to medical anomalies.

Cybersecurity: IoT devices have been particularly vulnerable to cyberattacks due to their widespread deployment and often minimal built-in security features [32].

GenAI-Enabled Autonomous and Intelligent IoT Systems

Generative Artificial Intelligence (GenAI) has emerged as a transformative paradigm in the evolution of autonomous systems, redefining how machines perceive, reason, and act within dynamic environments. Unlike traditional AI models that rely on static rule-based or discriminative learning approaches, GenAI focuses on the creation and simulation of new data patterns, enabling predictive adaptability and creativity in autonomous decision-making. Generative Artificial Intelligence (GenAI) has emerged as a transformative paradigm in the evolution of autonomous systems, redefining how machines perceive, reason, and act within dynamic environments [28][33]. Unlike traditional AI models that rely on static rule-based or discriminative learning approaches, GenAI focuses on the creation (as shown in Fig. 4) and simulation of new data patterns, enabling predictive adaptability and creativity in autonomous decision-making.



Fog.4 Genai-Enabled Autonomous and Intelligent Iot Systems

Smart-Home and Ambient Assisted Living: Smart-home applications illustrate the need for multimodal sensing rather than text-only interaction [34]. Ambient Assisted Living systems may combine data from Bluetooth beacons, cameras, wearable inertial sensors, motion sensors, door sensors, thermostats, power meters, and environmental sensors to infer context, activities, occupancy, safety risks, or anomalies.

Industrial IoT and Predictive Maintenance: In industrial IoT settings, LLMs can support predictive-maintenance workflows by summarizing sensor anomalies, maintenance logs, and operational constraints. Recent work on compressor monitoring shows how LLM-based predictive-maintenance frameworks can integrate heterogeneous sensor telemetry, maintenance reports, technical manuals, and operational context to support multimodal anomaly detection and maintenance decision support [35].

Smart Cities and Urban Intelligence: Smart-city applications require integration across traffic sensors, environmental monitoring, public-safety systems, energy grids, and citizen-facing services [36]. LLMs can support city operators by summarizing incidents, interpreting heterogeneous data sources, assisting emergency-response coordination, and explaining optimization decisions.

Digital Twins and Autonomous Agents: The usage of digital twins has several potential applications, including condition simulation, system status monitoring, and predictive analytics, as they offer virtual representations of actual systems. LLMs can enhance digital twins by enabling natural-language querying, explaining simulated outcomes, and orchestrating tool-based workflows.

Literature Review

This section highlights related studies on Generative Artificial Intelligence for Smart IoT Systems, emphasizing IoT-driven generative models, intelligent data processing, context-aware generation, smart healthcare, smart homes, energy management, personalization, and AI-enabled automation to improve the intelligence, efficiency, adaptability, security, and decision-making capabilities of modern IoT environments.

Subuhi Kashif Ansari et. al. (2026) discuss the integration of IoT data streams with AI architectures, including GANs and transformer-based models, for text-to-image generation. Real-time contextual and environmental information from IoT devices enhances image quality, contextuality, and personalization while addressing privacy and security concerns. Applications in smart homes, healthcare, and urban computing demonstrate its potential to improve user experiences and decision-making. Ethical and societal concerns, methods for integrating and fusing data from the Internet of Things, and AI models that are aware of their surroundings should all be the subject of future studies [37].

Ali Gunawan et. al. (2026) IoT is the fundamental data infrastructure, AI is used for making predictions and decision support, while generative AI enables personalization based on adaptive and narrative features. The high-profile problems of interoperability, data governance, ethics, and cybersecurity have not yet been addressed. The paper provides a comprehensive conceptual framework along with the identification of a research gap pertaining to scalable multimodal sensing, accountable AI governance, and a more inclusive multilingual interface for the advancement of sustainable tourism [38].

Surekha Lanka and Taipida Moodhitaporn (2025) present maintaining security enhancements for smart healthcare using federated learning. There securing the data of IoT -based sensors, which may lose local data while using smart systems. Removing this issue gives importance to local data also using the FL method. Thus, this research involves considering different research work and gives the research methodology for the security-enhancing process using FL in IoT-enhanced smart healthcare [39].

Vladimir Tsankov, Boris Evstatiev, and Irena Valova (2024) present a conceptual electronic household automation model that offers an affordable, multifunctional, and reliable solution for home management. Based on a microcomputer, the system collects and analyzes data while communicating with IoT devices. The proposed autonomous system can operate without Internet connectivity and aims to simplify smart-device management, optimize energy costs, and ensure household security and comfort [40].

Pavlo Beshley et. al. (2023) revealed limitations of existing SmartESS systems, including manual input, limited responsiveness to weather variations, and inadequate integration with smart home systems for energy-efficient household appliance management. To overcome these issues, modern IoT technologies were implemented with the Smart Life system for smart home control. A light sensor near the solar panels established a correlation between illumination (measured in lux) and solar power generation (measured in watts). Scenarios were then created in the Smart Life system to respond to changes in light intensity. High light levels automatically activate devices such as electric floor heating or ceramic heating panels, while decreased light levels switch them off, conserving general grid energy. This strategy enables real-time and efficient solar energy utilization [41].

Md. Ibne Joha, Md. Shafiul Islam and Shamim Ahamed (2022) present an IoT-based, intelligent control and protection system for home appliances using NodeMCU and Blynk app. System control and operation via the app are independent of the Wi-Fi network's nature. It eliminates the need for additional coding to connect the system to any Wi-Fi network, not just the home Wi-Fi. Moreover, it automatically detects and protects home appliances from overheating, overloading, gas leaks, and fire hazards. Furthermore, the dimmer circuit provides control over fan speed and light intensity. The system also provides a time-scheduling option and voice command control via Google Assistant. Above all, it saves energy and enhances human comfort [42].

Table I provides a summary of key studies on Generative Artificial Intelligence for Smart IoT Systems, highlighting their study focus, methodologies, key findings, challenges and limitations, and proposed future research directions across IoT-driven generative AI, smart healthcare, smart homes, sustainable applications, intelligent energy management, and AI-enabled home automation approaches.

Table 1 Comparative Analysis of Generative Artificial Intelligence for Smart IoT Systems

Reference	Study Focus	Approach	Key Findings	Challenges / Limitations	Future Directions
Subuhi Kashif Ansari et al. (2026)	IoT-driven generative AI for text-to-image generation	Integration of real-time IoT data streams with GANs and transformer-based models for text-to-image generation	IoT contextual and environmental data can improve image quality, contextual relevance, and personalization	Computational overhead, latency, privacy, and security issues associated with sensitive IoT data	Develop context-aware generative AI models, advanced IoT data fusion techniques, edge-based processing, and privacy-preserving approaches
Ali Gunawan et al. (2026)	Integration of IoT, AI, and generative AI for sustainable tourism	Conceptual framework combining IoT-based data collection, AI-based prediction and decision support, and generative AI for personalization	IoT acts as the data infrastructure, AI supports prediction and decision-making, and generative AI enables adaptive and personalized experiences	Interoperability, data governance, ethics, cybersecurity, and multilingual accessibility remain challenging	Develop scalable multimodal sensing, accountable AI governance, improved interoperability, and inclusive multilingual interfaces
Surekha Lanka and Taipida Moodhitaporn (2025)	Federated learning for secure IoT-based smart healthcare	Application of federated learning to protect IoT sensor data while enabling distributed model training without centralizing local data	Federated learning can improve privacy and security of IoT-enabled healthcare systems while preserving locally generated data	Local data loss, distributed data management, privacy, and security challenges	Develop robust federated learning frameworks with stronger data-preservation, privacy, and security mechanisms
Vladimir Tsankov, Boris Evstatiev and Irena Valova (2024)	IoT-based electronic household automation	Conceptual household automation system using a microcomputer for data collection, analysis, and communication with IoT devices	Provides affordable and multifunctional home automation while improving energy efficiency, security, comfort, and autonomous operation	Dependence on system hardware and limited connectivity options may restrict scalability and functionality	Integrate advanced intelligent automation, improved IoT connectivity, and more efficient smart-home management mechanisms
Pavlo Beshley et al. (2023)	IoT-enabled smart energy management in homes	Integration of IoT technologies, Smart Life system, and light sensors to monitor illumination and automatically control household appliances	Real-time monitoring of light intensity enables efficient solar-energy utilization and automatic appliance management	Existing SmartESS systems required manual input, had limited weather responsiveness, and lacked sufficient smart-home integration	Develop intelligent weather-aware automation, energy prediction, and deeper integration with smart-home ecosystems
Md. Ibne Joha, Md. Shafiul Islam and Shamim Ahamed (2022)	Intelligent IoT-based control and protection of home appliances	NodeMCU and Blynk-based control system with sensors, dimmer circuits, scheduling, and Google Assistant voice control	Enables automated appliance control, energy saving, comfort enhancement, and protection against overheating, overloading, gas leakage, and fire	Dependence on IoT hardware and communication infrastructure; protection mechanisms are mainly application-specific	Integrate AI-based intelligent control, predictive fault detection, advanced sensing, and broader smart-home interoperability

Conclusion and Future Work

Generative Artificial Intelligence is emerging as a transformative technology for enhancing the intelligence, adaptability, and autonomy of Smart IoT Systems. This review examined the foundations of IoT, including networking technologies, data-driven approaches, architectures, components, applications, and major challenges associated with heterogeneous devices, connectivity, scalability, and resource constraints. The integration of GenAI with IoT enables advanced capabilities such as synthetic data generation, intelligent data interpretation, predictive maintenance, personalized services, autonomous decision-making, and natural-language interaction. Edge-cloud and federated architectures provide promising approaches for reducing latency, preserving data privacy, and addressing computational limitations. Applications across smart homes, healthcare, industrial environments, smart cities, energy management, cybersecurity, and digital twins demonstrate the broad potential of GenAI-enabled IoT. However, challenges involving computational cost, interoperability, privacy, security, model reliability, and resource limitations remain significant. Overall, GenAI can strengthen IoT ecosystems by enabling more intelligent, context-aware, efficient, and autonomous systems while creating opportunities for innovative real-world applications.

Future research should focus on lightweight and energy-efficient generative models for resource-constrained IoT devices, privacy-preserving federated architectures, real-time edge inference, multimodal data fusion, and secure autonomous agents. Standardized benchmarks, explainable GenAI, robust security mechanisms, interoperability frameworks, and trustworthy human-AI collaboration are also essential for practical large-scale deployment.

References

[1] M. A. Naeem, T. N. Nguyen, R. Ali, K. Cengiz, Y. Meng, and T. Khurshaid, “Hybrid Cache Management in IoT-Based Named Data Networking,” IEEE Internet Things J., vol. 9, no. 10, pp. 7140–7150, 2022, doi: 10.1109/JIOT.2021.3075317.

[2] S. N. Koshy, I. F. B. Kamsin, and N. K. Zainal, “A Comprehensive Review on Smart IoT Applications,” 2021. doi: 10.2991/ahis.k.210913.069.

[3] N. Verma, S. Singh, and D. Prasad, “A Review on existing IoT Architecture and Communication Protocols used in Healthcare Monitoring System,” J. Inst. Eng. Ser. B, vol. 103, no. 1, pp. 245–257, 2022, doi: 10.1007/s40031-021-00632-3.

[4] M. Rahaman, “A Review on Internet of Things-IoT-Architecture, Technologies, Future Applications & Challenges,” Int. J. Sci. Bus., vol. 14, pp. 80–92, 2024, doi: 10.5281/zenodo.7066810.

[5] P. Patel, “Uncertainty-Aware Hybrid Deep Learning for AI-Generated vs Human Image Classification with Adaptive Human–AI Routing,” in 2026 2nd International Conference on Artificial Intelligence Systems (AIS), San Antonio, TX, USA: IEEE, May 2026, pp. 537–543. doi: 10.1109/AIS69919.2026.11621535.

[6] F. Mangione, C. Savaglio, and G. Fortino, “Generative Artificial Intelligence for Internet of Things Computing: A Systematic Survey,” Proc. Make sure to enter correct Conf. title from your rights confirmation email (Conference Acron. ’XX), vol. 1, no. 1, pp. 1–35, 2023.

[7] S. Madakam, R. Ramaswamy, and S. Tripathi, “Internet of Things (IoT): A Literature Review,” J. Comput. Commun., vol. 03, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.

[8] G. Islam and S. Motakabber, “A Comprehensive Review on the Internet of Things Network,” J. Commun., vol. 20, pp. 84–98, 2025, doi: 10.12720/jcm.20.1.84-98.

[9] M. R. Palattella et al., “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models,” IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 510–527, 2016, doi: 10.1109/JSAC.2016.2525418.

[10] M. Al-Sayed, “IoT Architecture for Smart Systems: A Data-Driven Approach to Machine Learning and Analytics,” Int. J. AI, Big Data, Comput. Manag. Stud., vol. 4, pp. 8–17, 2023, doi: 10.63282/3050-9416.IJAIBDCMS-V4I3P102.

[11] S. Singamsetty, “AI-Enabled Data Stewardship Real-Time Alignment of Privacy and Storage Policies Across Global Systems using Deep CNN-RNN Techniques,” in 2025 5th Asian Conference on Innovation in Technology (ASIANCON), PIMPRI, India: IEEE, 2025, pp. 1–6, August. doi: 10.1109/ASIANCON66527.2025.11281010.

[12] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, “An overview of IoT architectures, technologies, and existing open-source projects,” Internet of Things, vol. 20, p. 100626, Nov. 2022, doi: 10.1016/j.iot.2022.100626.

[13] R. Cheour, S. Khriji, M. Abid, and O. Kanoun, “Microcontrollers for IoT: Optimizations, Computing Paradigms, and Future Directions,” in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), IEEE, Jun. 2020, pp. 1–7. doi: 10.1109/WF-IoT48130.2020.9221219.

[14] A. Alawad and V. Marttin, “Internet of Things (IoT) and Smart Applications,” 2024, pp. 126–141.

[15] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and S. Uluagac, “A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications,” 2018, doi: 10.48550/arXiv.1802.02041.

[16] E. Faris Yahya and M. Mohammed, “The Challenges of Smart Environments and Future Trends Supported by the Internet of Things,” vol. 3, no. 3, pp. 528–534, 2023.

[17] A. Joon, “Smart Predictive Maintenance: AI-Driven Adaptation for Industrial Equipment,” in 2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECCE), IEEE, Jul. 2025, pp. 1–6. doi: 10.1109/NE-IECCE64154.2025.11183108.

[18] H. K. Yadav, “Design and Implement Machine Learning Based Predictive Analytics for Road Safety and Accident Prevention,” in 2026 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India: IEEE, 2026, pp. 1–6, March. doi: 10.1109/IATMSI68868.2026.11465965.

[19] B. Lima and R. Pinto, “Current Challenges and Future Perspectives in Testing IoT Systems: A Comprehensive Review,” IEEE Sensors Rev., vol. 3, pp. 22–47, 2025, doi: 10.1109/SR.2025.3628264.

[20] B. B. Gupta and M. Quamara, “An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols,” Concurr. Comput. Pract. Exp., vol. 32, no. 21, p. e4946, Nov. 2020, doi: 10.1002/cpe.4946.

[21] J. de Carvalho Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic, and A. L. L. Aquino, “LoRaWAN – A Low Power WAN Protocol for Internet of Things: A Review and Opportunities,”

in 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech 2017), 2017, pp. 1–6.
[22] G. Callebaut, G. Leenders, J. Van Mulders, G. Ottoy, L. De Strycker, and L. Van der Perre, "The Art of Designing Remote IoT Devices—Technologies and Strategies for a Long Battery Life," Sensors, vol. 21, no. 3, p. 913, Jan. 2021, doi: 10.3390/s21030913.
[23] N. Hussain, B. Austin, A. Ige, P. Adepoju, and A. Afolabi, "Generative AI advances for data-driven insights in IoT, cloud technologies, and big data challenges," Open Access Res. J. Multidiscip. Stud., vol. 6, pp. 51–59, 2023, doi: 10.53022/oarjms.2023.6.1.0040.
[24] H. Han, "Innovative Research on IoT Architecture and Robotic Operating Platforms: Applications of Large Language Models and Generative AI," in 2024 6th International Conference on Robotics, Intelligent Control and Artificial Intelligence (RICAI), IEEE, Dec. 2024, pp. 881–887. doi: 10.1109/RICAI64321.2024.10911316.
[25] U. Tiwari, "Generative AI for Smart IoT Systems," vol. 1, no. 2, pp. 133–147, 2025.
[26] K. K. Mohammed, "The Future is Cloud : Modernizing Big Data for the Cloud Era," Int. J. Sci. Res. Eng. Trends, vol. 11, no. 5, pp. 1–5, 2025.
[27] K. Jangiti, "Design and Validation of a Machine Identity Governance Framework for AI Agents in Multi-Cloud Environments," in SoutheastCon 2026, Huntsville, AL, USA: IEEE, 2026, pp. 1–6, February-March. doi: 10.1109/SoutheastCon63549.2026.11476363.
[28] L. Marathe, S. Moharana, S. Nayak, and P. Sahu, "Intelligent Autonomous Robotics System with IoT and Generative AI for Smart Environment Management," IJARCCE, vol. 14, 2025, doi: 10.17148/IJARCCE.2025.141132.
[29] X. Wang et al., "The Internet of Things in the Era of Generative AI: Vision and Challenges," IEEE Internet Comput., vol. 28, pp. 57–64, 2024, doi: 10.1109/MIC.2024.3443169.
[30] S. Desai, "Multi-Layered Memory Architecture for Institutional Intelligence: A Technical Implementation Guide," J. Comput. Anal. Appl., vol. 34, no. 12, pp. 986–1005, August, 2025, doi: 10.48047/jocaaa.2025.34.12.81.
[31] X. Wang, Z. Wan, A. Hekmati, M. Zong, and S. Alam, "IoT in the Era of Generative AI : Vision and Challenges," pp. 1–15.
[32] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," Computer (Long. Beach. Calif)., vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.
[33] N. Bhandarwar, "Integrating Generative AI and Model Context Protocol (MCP) with Applied Machine Learning for Advanced Agentic AI Systems," Int. J. Comput. Trends Technol., vol. 73, no. 8, pp. 7–14, August, Aug. 2025, doi: 10.14445/22312803/IJCTT-V73I8P102.
[34] S. Ahmadzadeh and G. Karthick, "Large Language Models for Future Internet Ecosystems: A Taxonomy-Based Review of Smart IoT, Edge Intelligence, and Autonomous AI," pp. 1–23, 2026.
[35] G. Palma, G. Cecchi, and A. Rizzo, "Large Language Models for Predictive Maintenance in the Leather Tanning Industry: Multimodal Anomaly Detection in Compressors," 2025.
[36] K. M. Hussain and S. C. Pallaprolu, "Improving Passenger Safety with Machine Learning Techniques on 2022 Incident Data," in 2025 International Conference on Sensors and Related Networks (SENNET) Special Focus on Digital Healthcare (64220), Vellore, India: IEEE, 2025, pp. 1–6, July. doi: 10.1109/SENNET64220.2025.11136102.
[37] S. K. Ansari, N. Hamid Shah, M. A. Hussain, R. Fayaz, A. U. Begum, and D. T. Khan, "IoT-Enabled Text-to-Image Generation: A Review of Artificial Intelligence and Machine Learning Approaches," in 2026 1st International Conference on Emerging Technologies and Engineering Systems (ICETES), 2026, pp. 15–20. doi: 10.1109/ICETES68504.2026.11518593.
[38] A. Gunawan, R. Wiputra, M. I. Wijaya, R. Widuri, and M. M. Ali, "IoT, AI, and Generative AI in Smart Tourism: A Systematic Literature Review Using PRISMA," in 2026 International Conference on Connected Intelligence for Industrial Applications (CI2A), 2026, pp. 1–7. doi: 10.1109/CI2A69097.2026.11576776.
[39] S. Lanka and T. Moodhitaporn, "IoT Security Enhancements in Smart Healthcare Using Federated Learning," in 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), 2025, pp. 263–267. doi: 10.1109/ICSADL65848.2025.10933330.
[40] V. Tsankov, B. Evstatiev, and I. Valova, "Concept for an IoT-based Electronic System for Smart Home Automation," in 2024 9th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE), 2024, pp. 1–5. doi: 10.1109/EEAE60309.2024.10600500.
[41] P. Beshley, M. Kaidan, B. Strykhalyuk, O. Kochan, S. Mokhun, and O. Fedchyshyn, "IoT Empowered SmartESS Systems for Real-Time Monitoring and Control in Smart Grid," in 2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT), 2023, pp. 1–5. doi: 10.1109/AICT61584.2023.10452690.
[42] M. Ibne Joha, M. Shafiul Islam, and S. Ahamed, "IoT-Based Smart Control and Protection System for Home Appliances," in 2022 25th International Conference on Computer and Information Technology (ICCIT), 2022, pp. 294–299. doi: 10.1109/ICCIT57492.2022.10054941.