Discover Internet of Things

Review

A review on WSN based resource constrained smart IoT systems

Shreeram Hudda[1] · **K. Haribabu**[1]

Received: 16 February 2025 / Accepted: 15 April 2025
Published online: 09 May 2025

Abstract
In Wireless Sensor Network (i.e. WSN) based resource constrained Internet of Things (i.e. IoT) environments, efficient data forwarding is achieved through cluster based mechanisms, where cluster heads facilitate communication among themselves and with the sink node. Data collected by each cluster head is temporarily buffered before being transmitted to the sink via multi-hop communication. The integration of advanced wireless technologies, such as 5th Generation (i.e. 5G) networks, offers significant benefits, including reduced latency, extensive coverage, improved spectral efficiency, and higher data transmission rates. Incorporating Device-to-Device (i.e. D2D) communication further enhances energy efficiency and offloads data traffic, addressing critical IoT requirements such as low latency, increased network capacity, and improved spectral and energy efficiency. Software Defined Networking (i.e. SDN) addresses diverse IoT network needs across domains like smart grids, healthcare, traffic signaling, agriculture, and smart homes by enabling efficient communication, network management, and innovative control procedures. However, SDN's application for anomaly detection and primary defense against security threats in IoT systems remains underexplored. This research investigates the potential of the design of an intelligent mechanism for energy efficient, privacy preserving, and secure communication in WSN based resource constrained IoT systems. The proposed approach leverages advanced technologies such as SDN, Machine Learning (i.e. ML), Deep Learning (i.e. DL), D2D communication, Computer Vision, and Network Function Virtualization (i.e. NFV). Additionally, it emphasizes assessing and offloading specific IoT application functions onto the network's edge to enhance performance. Moreover, the development of lightweight security mechanisms for secure communication in resource constrained IoT environments is also identified as a crucial research domain.

Article Highlights

- Despite the presence of numerous frameworks and architectures for smart IoT systems, a standardized framework and architecture is still missing, often neglecting security and privacy aspects.
- Cluster head selection highlights a gap and suggests the potential for developing an energy efficient mechanism by incorporating additional parameters.
- There is a demand for lightweight cryptosystems to provide security and protect privacy in smart IoT networks.

Keywords Smart system · WSN · IoT · Clustering · Cluster head · Energy efficiency · Privacy preserving · Security · Computer vision · SDN · 5G · D2D communication · Edge computing · ML · DL

✉ Shreeram Hudda, p20200471@pilani.bits-pilani.ac.in; K. Haribabu, khari@pilani.bits-pilani.ac.in | [1]SDN Lab, Department of Computer Science and Information Systems, Birla Institute of Technology & Science - Pilani (BITS-Pilani), Pilani Campus, Pilani, Rajasthan 333031, India.

1 Introduction

1.1 Wireless sensor network

A Wireless Sensor Network (i.e. WSN) [1–4] is a network of spatially distributed, autonomous sensor nodes that communicate wirelessly to monitor physical or environmental conditions such as temperature, humidity, pressure, motion, light, or pollutants [3]. These sensor nodes collect and transmit data to a central base station for further processing and analysis. The functionality of a WSN is driven by its key components [1], including sensor nodes, microcontrollers, wireless communication modules, power sources, and a base station. Each component plays a critical role in ensuring seamless data acquisition, processing, transmission, and decision making. The following are the key components of a sensor node:

1. Sensor Nodes: Sensor nodes form the fundamental building blocks of a WSN [1]. Each node consists of multiple components that work together to sense, process, and transmit data. These nodes are typically deployed in large numbers, making the network scalable and efficient for monitoring vast areas. The basic components of a sensor node are shown in figure 1. WSNs are composed of spatially distributed small sensor nodes that monitor and collect data from their environment. These nodes are designed to operate autonomously, communicate wirelessly, and work collectively to transmit the gathered information to a central location for further analysis.
2. Microcontroller: Once the raw sensor data is collected, it is processed by the microcontroller (i.e. processing unit), which acts as the brain of the sensor node [1]. The microcontroller filters noise, processes relevant information, and determines whether the data should be transmitted immediately or stored for later use. Efficient processing is crucial for reducing unnecessary data transmission, thereby conserving energy and improving network longevity. At the core of a WSN lies the ability to sense and collect data from its environment. Each sensor node is equipped with one or more sensors that detect changes in physical parameters such as temperature, humidity, motion, light intensity, or pressure. The collected data is often in analog form, may require conversion into digital signals before further processing. For instance, in a smart agriculture system, soil moisture sensors measure the water content in the soil, allowing farmers to optimize irrigation schedules. Similarly, in healthcare applications, wearable sensor nodes monitor heart rate and body temperature to track patient health in real time. The accuracy and efficiency of these sensors directly influence the overall performance of the WSN.
3. Communication Module: The communication module enables seamless data transmission between nodes and to the base station [1]. These modules vary based on the type of network protocol being used. For instance, Zigbee is preferred for low power applications, whereas Wi-Fi is suitable for high speed data transfer. Efficient communication protocols ensure reliable data delivery while minimizing power consumption. The ability of WSNs to function wirelessly is one of their most defining features. Sensor nodes communicate with one another and with the base station using wireless communication protocols such as Zigbee, Bluetooth, Wi-Fi, LoRa, or 6LoWPAN. The choice of protocol depends on the specific application, with considerations such as power consumption, range, and data transfer speed playing key roles. When a sensor node gathers and processes data, it transmits this information to the nearest node or directly to the base station. Depending on the network topology, the data may pass through multiple relay nodes

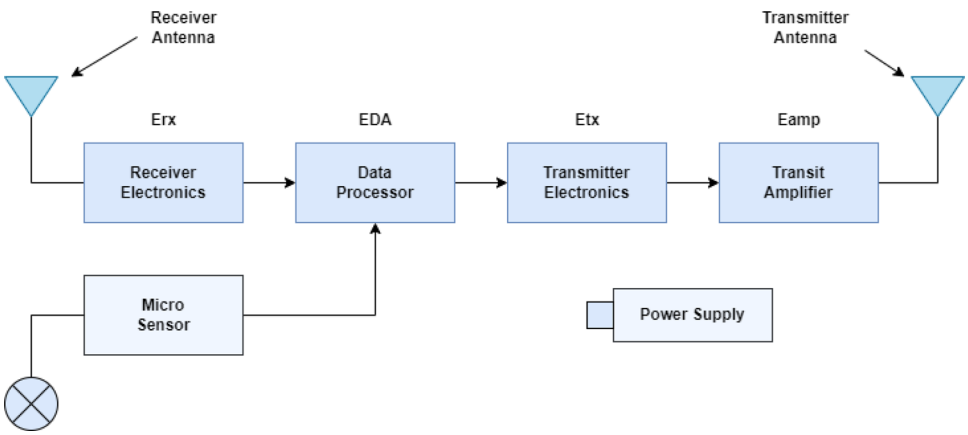


Fig. 1 Key components of a sensor node [5]

before reaching its final destination. The base station then forwards the aggregated data to a remote server or cloud system, where further analysis and decision making take place.

4. Power Source: The power source provides the necessary energy for all components of a sensor node to function [1]. Batteries are commonly used, but energy harvesting techniques such as solar panels or wind panels can be integrated to enhance longevity. Choosing the right power source is crucial for maintaining reliable network performance. One of the most critical challenges in WSN design is power management. Since sensor nodes are often deployed in remote or inaccessible locations, replacing or recharging their batteries is difficult. Therefore, energy efficiency is a key consideration in WSN deployment. For instance, in environmental monitoring applications, sensor nodes may only wake up at specific intervals to collect data, transmit it, and then return to a low power sleep mode. This approach significantly conserves battery life and enhances the long term sustainability of the WSN. To extend the network's lifespan, various energy saving techniques are employed, including:
    - Duty cycling: Where nodes alternate between active and sleep modes to reduce power consumption.
    - Energy harvesting: Renewable energy sources such as solar or wind can be used to recharge sensor node batteries.
    - Efficient data transmission protocols: Efficient data transmission protocols minimize redundant communication and optimize network traffic.

5. Sink Node: The sink node[1] plays a crucial role in collecting, processing, and forwarding sensor data to external systems [1]. It serves as the interface between the WSN and the internet or cloud services. Since the base station often has a more powerful processor and an unlimited power source, it can perform advanced data processing and decision making tasks. After sensor nodes collect and transmit data, it reaches the base station, also known as the sink node. The base station serves as a central hub that gathers information from multiple sensor nodes, processes the data, and forwards it to a remote server or cloud platform for further analysis. In large scale WSNs, data aggregation techniques are used to minimize redundancy and reduce the amount of data transmitted over the network. By summarizing and compressing similar data, the network conserves bandwidth and energy while ensuring relevant information is retained. For example, in smart city applications, a WSN may collect air quality data from various locations. Instead of transmitting all raw sensor readings, the base station can aggregate the data by calculating average pollution levels, trends, and anomalies before sending a summarized report to city authorities.

As stated earlier, WSNs consist of interconnected sensor nodes that monitor environmental conditions, process data, and transmit information to a central system for analysis. The operation of WSNs involves multiple key components working collaboratively to ensure efficient data collection, processing, and transmission [3]. Below is a detailed breakdown of how these components interact [3], and the same is placed in figure 2:

- Sensing: The fundamental role of sensor nodes is to detect and measure environmental changes such as temperature fluctuations, humidity levels, light intensity, motion, pressure, or chemical concentrations. Each sensor node is equipped with one or more sensing units that continuously monitor the surrounding environment. When a significant change occurs, the sensor captures the raw data and prepares it for further processing.
- Data Processing: Once the sensor collects data, it is passed to the microcontroller or processing unit of the sensor node. The microcontroller filters and processes the raw data, removing noise and redundant information to ensure only relevant and meaningful data is retained. This step helps optimize power consumption and reduces the amount of data that needs to be transmitted, thereby enhancing the efficiency of the WSN.
- Data Transmission: After processing, the refined data is transmitted wirelessly to the sink node using a wireless communication module. This module typically employs communication protocols such as Zigbee, Bluetooth, LoRa, or Wi-Fi, depending on the network's requirements. The sensor nodes may communicate directly with the sink node (i.e. single hop communication) or relay data through intermediate nodes (i.e. multi-hop communication) to extend the network's coverage.
- Data Aggregation: The sink node plays a crucial role in collecting and aggregating data from multiple sensor nodes. It consolidates data from various sources, eliminates duplicate readings, and applies further filtering techniques to

[1] The words base station and sink node will be used interchangeably throughout this work.

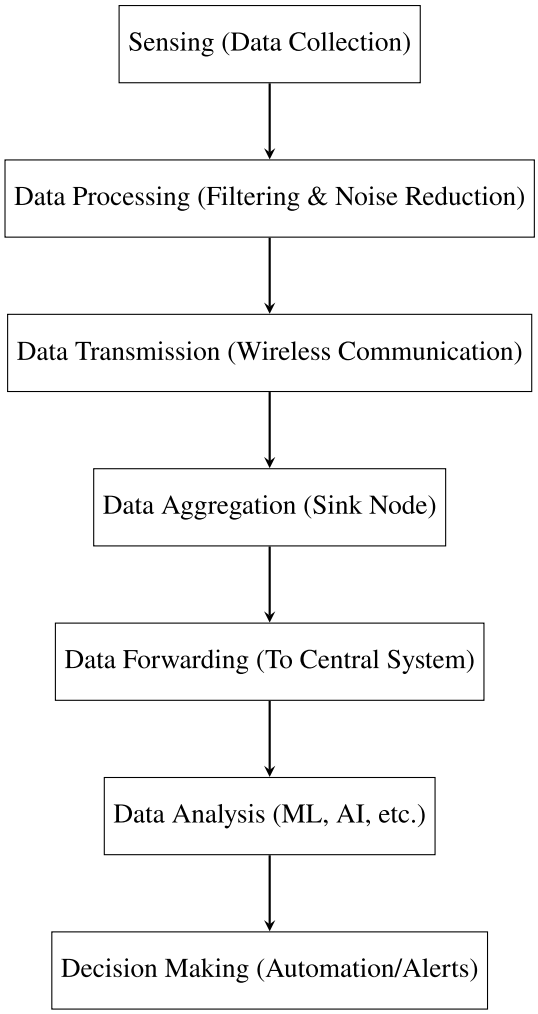


Fig. 2 Flowchart for how WSN and Its components work together

improve data accuracy and minimize transmission overhead. This aggregation process helps in reducing network congestion and optimizing energy efficiency.

- Data Forwarding and Analysis: After aggregation, the sink node forwards the processed data to a central system, such as a cloud server, edge computing device, or control center. The central system performs in-depth analysis using machine learning (i.e. ML) algorithms, data analytics tools, or artificial intelligence to extract valuable insights. Based on the analysis, decisions can be made for automated responses, alerts, or further actions, such as adjusting environmental controls, triggering alarms, or sending notifications to users.

This coordinated process enables WSNs to function effectively in applications such as environmental monitoring, healthcare, smart cities, industrial automation, and precision agriculture. The seamless integration of sensing, processing, communication, and analysis ensures reliable data driven decision making across various domains.

1.1.1 Advantages of WSNs

WSNs offer numerous benefits that make them essential for various applications, including environmental monitoring, healthcare, industrial automation, and smart cities [3, 4]. However, they also come with certain limitations that affect their performance and reliability. Below is a detailed discussion of the advantages of WSNs. Several of these advantages are stated below:

- Scalability: WSNs are highly scalable, allowing for the easy expansion of the network by adding additional sensor nodes as needed. This flexibility enables WSNs to support growing applications, whether in large industrial environments, urban infrastructure, or agricultural monitoring. The ability to scale without significant infrastructure modifications makes WSNs a cost effective solution for dynamic environments.
- Remote Monitoring and Real Time Data Collection: One of the most significant advantages of WSNs is their ability to monitor remote or hazardous locations without requiring human intervention. Sensor nodes can be deployed in inaccessible areas, such as deep sea environments, industrial zones, or disaster stricken regions, to collect real time data. This enables timely decision making and enhances situational awareness in critical applications.
- Cost Effectiveness: Compared to traditional wired sensor networks, WSNs significantly reduce the costs associated with installation, maintenance, and infrastructure. Wired networks require extensive cabling, which can be expensive and difficult to install, particularly in large scale or remote deployments. In contrast, WSNs eliminate the need for physical connections, reducing both material and labor costs.
- Support for IoT Applications: WSNs play a vital role in the Internet of Things (i.e. IoT) ecosystem by enabling seamless communication between smart devices. They facilitate data collection and transmission for various IoT based applications, including smart cities (e.g., traffic monitoring, smart lighting), healthcare (e.g., wearable medical devices, remote patient monitoring), and industrial automation (e.g., predictive maintenance, smart factories). This integration enhances efficiency, automation, and data driven decision making across multiple sectors.

1.1.2 Challenges in WSNs

Despite of numerous advantages of WSNs, they also face several critical challenges that impact their performance, reliability, and scalability [3, 4]. Addressing these challenges is essential for enhancing the efficiency and sustainability of WSN deployments. Some of these challenges are listed below:

- Limited Energy Resources: Sensor nodes in WSNs are typically powered by small batteries with limited energy capacity. Since many WSNs are deployed in remote or inaccessible locations, frequent battery replacements are impractical. Energy efficiency remains a major concern, requiring optimized power management strategies, such as duty cycling, low power communication protocols, and energy efficient hardware design.
- Security Risks: WSNs are vulnerable to various cyber threats, including unauthorized access, data interception, denial-of-service (i.e. DoS) attacks, and node tampering. Due to their wireless nature and resource constrained hardware, implementing robust security measures, such as encryption, authentication, and intrusion detection systems, is challenging but essential for protecting data integrity and network reliability.
- Interference and Data Loss: Wireless communication in WSNs is susceptible to interference from other electronic devices, environmental obstacles, and signal attenuation. Factors such as electromagnetic interference, multipath fading, and congestion can lead to packet loss, reduced transmission range, and unreliable data delivery. Advanced signal processing techniques and adaptive communication protocols can help mitigate these issues.
- Data Reliability in Harsh Environments: WSNs deployed in extreme conditions-such as industrial sites, underwater monitoring, or disaster prone areas face additional challenges like sensor failures, hardware degradation, and harsh environmental conditions (e.g., extreme temperatures, humidity, or physical obstructions). Ensuring consistent data reliability requires redundant sensor deployment, error correction techniques, and fault tolerant network architectures.
- Limited Processing and Storage Capabilities: Sensor nodes in WSNs are typically designed with minimal computational power and memory capacity to reduce energy consumption. While this helps prolong battery life, it also limits their ability to perform complex data processing and storage tasks. To overcome this constraint, WSN architectures often incorporate edge computing and cloud based processing, where data analysis is performed at more powerful computing nodes.
- Scalability and Network Management Challenges: Managing large scale WSNs presents significant challenges in terms of network topology, data synchronization, and resource allocation. As the number of sensor nodes in a WSN increases, managing network resources, routing data efficiently, and maintaining connectivity become more complex. Large scale WSNs require robust self organizing mechanisms, optimized data aggregation techniques, and efficient routing algorithms to prevent congestion and ensure smooth communication.

1.2 Internet of things

The Internet of Things (i.e. IoT) is a vast ecosystem of interconnected physical devices that collect, process, and exchange data over the Internet without human intervention [6, 7]. These devices, embedded with sensors, software, and network connectivity, communicate in real time to enhance automation, efficiency, and decision making in various domains. IoT plays a crucial role in smart homes, healthcare, industrial automation, agriculture, smart cities, and environmental monitoring. Moreover, figure 3 represents the tri-sectional relationship among three aspects of IoT [8]: (a) humans, (b) objects, and (c) internet.

IoT systems consist of several key components that work together to enable seamless data collection, processing, and transmission [6, 9, 10]. Each component plays a significant role in ensuring the smooth operation of IoT based applications. The main key components of IoT are:

1. Sensors and Actuators: IoT devices rely on sensors and actuators to interact with the physical world. Sensors collect real time data from the environment, while actuators respond to this data by triggering physical actions, enabling smart and automated decision making
2. Connectivity Module: For an IoT system to function effectively, its devices must communicate with each other and with cloud platforms. This is achieved through various wireless and wired connectivity technologies. The connectivity module ensures seamless communication between IoT devices, gateways, and cloud platforms, enabling remote monitoring and control
3. Edge and Cloud Computing: IoT devices generate massive amounts of data that need to be processed efficiently. Edge computing and cloud computing work together to handle this data. Edge computing ensures real time processing, while cloud computing provides large scale data storage and analytics capabilities, making IoT systems more efficient and scalable
4. User Interface: IoT applications require user interfaces (i.e. UIs) that allow individuals to monitor and control devices. User interfaces help end users to interact with IoT devices, providing control, monitoring, and data visualization in a user friendly way

The IoT operates through a structured workflow that enables seamless data collection, transmission, processing, and action, allowing devices to function autonomously while providing real time insights [6, 9, 10]. As mentined previously, the IoT ecosystem comprises interconnected devices, sensors, actuators, communication networks, and data processing platforms, all working together to automate processes and improve efficiency. Below is a detailed breakdown of the IoT workflow and the same is presented in figure 4:

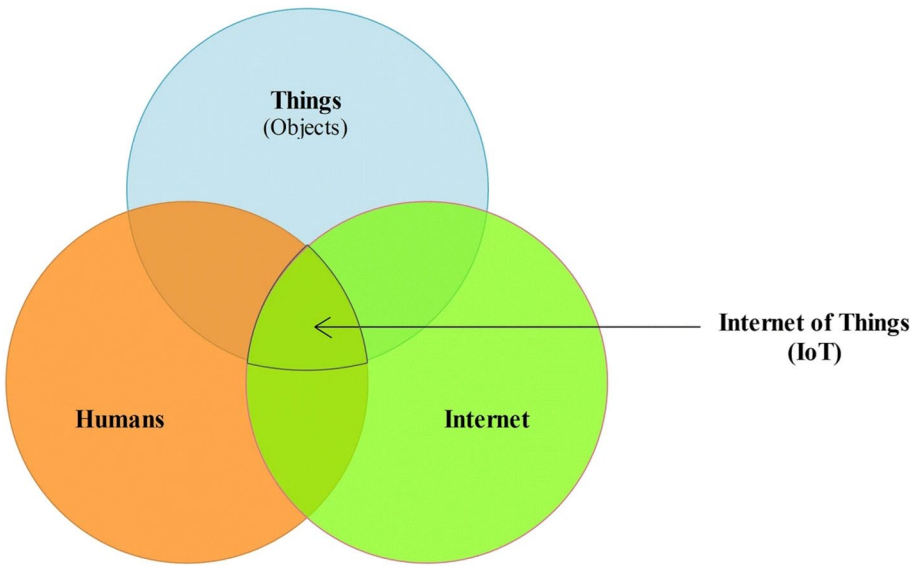


Fig. 3 Tri-Sectional Relationship Among Three Aspects of IoT [8])

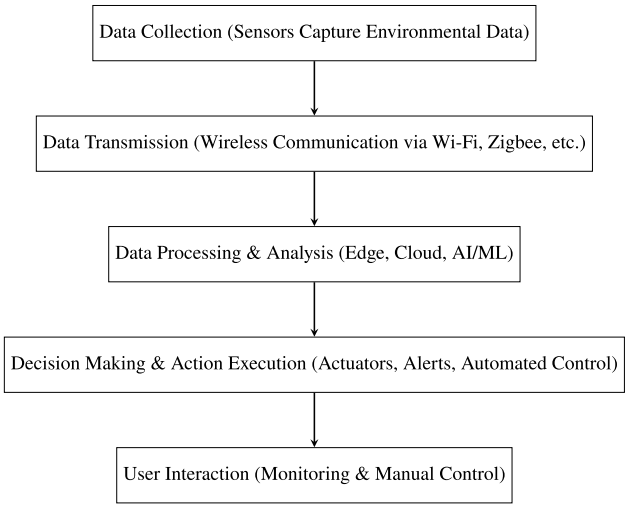


Fig. 4 Flowchart for How IoT and Its Components Work Together

- Data Collection: The IoT begins with data collection through various sensors embedded in connected devices. These sensors are designed to detect and measure environmental conditions such as temperature, humidity, pressure, motion, light levels, gas concentrations, or object proximity. Sensors continuously monitor their surroundings and capture raw data, which is then may be converted into a digital format for processing. The frequency of data collection depends on the application-some systems collect data at regular intervals, while others operate in response to specific triggers. For instance, a temperature sensor installed in a smart home continuously measures room temperature and records fluctuations in real time.
- Data Transmission: Once data is collected, it must be transmitted to a processing unit, such as an edge device or cloud server, for analysis. IoT devices use various communication protocols to transmit data, including Wi-Fi, Bluetooth, Zigbee, LoRa, and cellular networks (e.g., 4G/5G). The connectivity module within an IoT device ensures seamless communication with a local gateway, edge computing device, or cloud platform. The choice of communication technology depends on factors such as power consumption, data volume, and network coverage. For instance, a smart temperature sensor in a home automation system sends real time temperature readings to the cloud using a Wi-Fi connection.
- Data Processing and Analysis: After data reaches the processing unit, it undergoes analysis to extract meaningful insights and identify patterns or anomalies. Depending on the application, data processing can take place at different levels:

  – Edge Computing: In scenarios requiring low latency (e.g., industrial automation, healthcare monitoring), edge devices process data locally before sending it to the cloud. This reduces transmission delays and optimizes real time decision making.
  – Cloud Computing: For large scale data analysis, cloud servers aggregate data from multiple IoT devices and apply advanced analytics, including artificial intelligence (i.e. AI) and ML algorithms, to detect trends, predict future outcomes, and optimize system performance.

  For example, in a smart building, the IoT system analyzes temperature data from multiple rooms. If it detects a continuous rise in temperature beyond the preset threshold, it triggers the next step.
- Decision Making and Action: Based on the processed data, the IoT system makes automated decisions and triggers appropriate actions through actuators or control mechanisms. Actuators are physical components that convert digital commands into real world actions, such as turning on appliances, adjusting machinery, or sending alerts. The system applies predefined rules or AI driven decision models to determine the necessary response. This could involve direct automation or alerting human operators for intervention. For example, if the IoT system detects that the room temperature has exceeded a set limit, it automatically sends a command to turn on the air conditioning unit. In industrial settings, IoT enabled machines can automatically adjust operating parameters to prevent overheating or equipment failure.

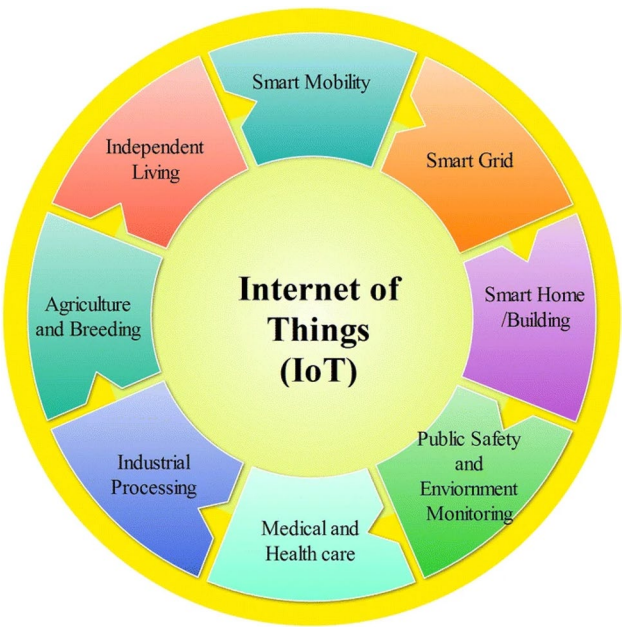
- User Interaction: While many IoT systems operate autonomously, users can also interact with connected devices through mobile apps, dashboards, or web based interfaces. These interfaces allow users to monitor real time data, customize settings, and manually control IoT devices if needed. The IoT platforms provide visualization tools and control mechanisms that enable users to track device status, receive notifications, and override automated decisions when necessary. For instance, a homeowner can use a smartphone app to check the room temperature and manually adjust the thermostat, even when they are away from home. In smart factories, operators can use a dashboard to monitor machine performance and adjust settings remotely.

1.2.1 Applications of IoT

The use of IoT has significantly transformed various industries by enabling real time data collection, automation, and intelligent decision making [9, 11–15]. With the integration of cloud computing, and AI, IoT applications are driving efficiency, sustainability, and innovation. From monitoring environmental conditions to enhancing healthcare and optimizing industrial operations, IoT plays a pivotal role in improving processes and services across multiple domains. The IoT networks are used for various applications, such as environmental monitoring, healthcare, smart cities, industrial automation, and military surveillance. Several application areas of IoT have been depicted in figure 5. Below are some key areas where IoT is making a substantial impact [9, 11–15]:

- Environmental Monitoring: IoT technology plays a crucial role in tracking and analyzing environmental conditions. It is widely used in climate change studies to collect real time data on temperature variations, humidity levels, and greenhouse gas emissions. Disaster prediction systems leverage IoT sensors to monitor seismic activity, weather patterns, and flood risks, enabling early warning mechanisms. Additionally, pollution control initiatives utilize IoT enabled air and water quality sensors to detect harmful pollutants, ensuring timely interventions to protect public health.
- Healthcare: The integration of IoT in healthcare has led to significant advancements in patient care and medical monitoring. Remote patient monitoring systems use IoT enabled devices to track vital signs such as heart rate, blood pressure, and glucose levels, transmitting real time data to healthcare professionals for timely diagnosis and intervention. Wearable health devices, including smartwatches and fitness trackers, provide continuous health monitoring, promoting preventive care and personalized treatment plans for patients with chronic conditions.
- Smart Cities: IoT solutions contribute to the development of smart cities by optimizing urban infrastructure and services. Traffic monitoring systems use IoT sensors and cameras to analyze vehicle movement, manage congestion, and enhance road safety. Smart street lighting systems adjust brightness based on real time pedestrian

Fig. 5 Applications of IoT [8]



and vehicle presence, reducing energy consumption. Additionally, IoT based waste management solutions employ smart bins equipped with sensors to detect fill levels, ensuring efficient waste collection and disposal.

- Agriculture: IoT driven solutions in agriculture enhance productivity and resource efficiency. Soil moisture sensors provide real time data on soil conditions, allowing farmers to optimize irrigation schedules and conserve water. Smart irrigation systems automate water distribution based on environmental conditions, reducing wastage and improving crop yields. IoT technology also aids in precision farming by monitoring weather patterns, soil health, and pest infestations, enabling data driven decision making.
- Industrial IoT: The implementation of IoT in industrial environments has revolutionized manufacturing and maintenance operations. Smart factories use IoT enabled machinery and sensors to optimize production processes, minimize downtime, and enhance efficiency. Predictive maintenance leverages IoT data analytics to monitor equipment health, detect anomalies, and schedule maintenance proactively, preventing unexpected failures and reducing operational costs.
- Transportation and Logistics: The IoT is revolutionizing the transportation and logistics industry by providing real time tracking, automated fleet management, and predictive maintenance for vehicles. By integrating IoT enabled sensors, GPS tracking systems, and advanced data analytics, companies can optimize operations, reduce costs, enhance safety, and improve overall efficiency.
- Smart Homes: IoT assists home automation by enabling homeowners to remotely monitor, control, and automate various household devices, improving comfort, security, and energy efficiency. Through interconnected smart devices such as lighting systems, thermostats, security cameras, and smart locks, IoT provides seamless automation and real time control using mobile apps, voice assistants, and cloud based platforms.

1.3 WSNs assist IoT

WSNs play a crucial role in the IoT by facilitating efficient data collection, communication, and decision making. A WSN consists of multiple sensor nodes that monitor environmental conditions, process collected data, and transmit it wirelessly to IoT platforms for further analysis and automation. The WSN networks form the backbone of various IoT applications by ensuring real time data acquisition, low power operation, secure communication, and seamless connectivity, even in remote areas [16–19]. WSNs assist IoT in several ways, including:

- Real Time Data Collection: WSNs provide IoT systems with continuous, real time data from a network of distributed sensors deployed in diverse environments. These sensors measure physical parameters such as temperature, humidity, pressure, motion, and air quality, providing the necessary input for IoT based decision making systems.
  - How it Works: Each sensor node within the WSN captures environmental data and transmits it wirelessly to a central gateway or cloud based IoT platform. Advanced data fusion techniques ensure that real time insights are derived from multiple sensor readings.
  - Example: In precision agriculture, IoT enabled smart farming systems use temperature and humidity sensors deployed across agricultural fields to monitor soil moisture levels. The collected data is transmitted to an IoT platform, where automated irrigation systems adjust water distribution accordingly, optimizing resource usage and improving crop yield.
- Connectivity in Remote and Hard to Reach Areas: WSNs enable IoT applications in rural, mountainous, underwater, or other remote areas where traditional wired or cellular internet infrastructure is unavailable or unreliable. By forming self organizing mesh networks, sensor nodes can relay data over long distances without requiring direct internet access.
  - How it Works: Sensor nodes use multi-hop communication to pass data from one node to another until it reaches a central gateway or satellite uplink, ensuring continuous connectivity.
  - Example: IoT powered wildlife monitoring systems use WSNs to track animal movements in forests, national parks, and conservation areas. GPS enabled sensor collars on animals send tracking data to nearby WSN nodes, which relay the information to cloud based analytics platforms, enabling to study migration patterns and protect endangered species.

- Data Aggregation and Preprocessing: WSNs play a vital role in optimizing IoT data transmission by aggregating and preprocessing sensor data before sending it to cloud based systems. This approach reduces network congestion, minimizes bandwidth usage, and ensures efficient data management.

  - How it Works: Edge based WSN nodes perform local processing, filtering, and aggregation of raw sensor data, transmitting only essential or meaningful information to IoT platforms.
  - Example: In industrial IoT applications, edge based WSN nodes monitor factory conditions (e.g., temperature, vibration, and air quality). Instead of sending all raw sensor readings, the nodes preprocess the data and only transmit significant changes or anomalies, reducing network load and improving response times.

- Energy Efficient Communication: WSNs are designed to operate with minimal power consumption, making them ideal for IoT applications where sensor nodes are often deployed in remote or inaccessible locations. They utilize energy efficient communication protocols such as Zigbee, LoRaWAN, and Bluetooth to extend battery life and maintain long term operations.

  - How it Works: WSN nodes use optimized data transmission schedules and low power radio communication to reduce energy consumption. Some systems employ energy harvesting techniques (e.g., solar power) to enhance sustainability.
  - Example: Smart water meters in residential and commercial buildings use WSNs to periodically transmit water usage data to IoT based billing systems. By employing low power communication protocols, these meters can function for years without requiring frequent battery replacements.

As stated earlier, the WSNs serve as a fundamental building block of IoT ecosystems by enabling seamless data collection, energy efficient communication, and reliable connectivity in remote areas. Their integration with IoT applications enhances automation, optimizes resource management, and ensures real time monitoring across industries such as agriculture, healthcare, smart cities, industrial automation, and environmental monitoring.

While WSNs significantly enhance IoT functionality in many applications, their effectiveness depends on various factors, including energy efficiency, data transmission reliability, security, and scalability. Some applications benefit immensely from WSN integration, while others face challenges due to WSN limitations [16–19]. In numerous IoT applications, WSNs offer substantial advantages, particularly in real time monitoring, data collection, low power wireless communication, and cost effective deployment. Their ability to function in remote and challenging environments makes them an essential component of IoT ecosystems [16–19]. Due to the following reasons the WSNs provide adequate assistance:

1. Real Time Data Collection: WSNs ensure continuous, real time data collection from a vast network of sensor nodes, enabling IoT systems to function autonomously and respond dynamically to changing conditions. This real time monitoring capability is particularly valuable in applications that require instant decision making and automation. For example, in precision agriculture, WSNs collect temperature, humidity, and soil moisture data in real time. The data is processed and sent to an IoT platform, which automatically adjusts irrigation levels to optimize water usage and improve crop yield.
2. Scalability for Large Scale IoT Networks: WSNs support the deployment of thousands of interconnected sensor nodes, making them ideal for large scale IoT applications. Their self organizing capabilities enable seamless network expansion without requiring significant modifications. For instance, in smart cities, WSNs facilitate large scale air pollution monitoring. Thousands of sensor nodes deployed across urban areas collect data on CO_2, NO_2, and particulate matter, relaying the information to a central IoT platform that helps authorities implement pollution control measures.
3. Cost Effectiveness in Remote and Harsh Environments: Compared to traditional wired infrastructure, WSNs offer a cost effective solution for IoT deployments in rural, industrial, and hazardous locations. Eliminating the need for physical cables reduces installation costs and allows for flexible deployment. For example, in the oil and gas industry, WSNs monitor pipeline pressure, temperature, and leak detection in remote locations. Deploying wired sensors over long distances would be costly and impractical, whereas WSNs provide a reliable and affordable alternative.
4. Efficient Communication for IoT Devices: WSNs employ low power wireless communication protocols, such as Zigbee, LoRaWAN, Bluetooth, and 6LoWPAN, to extend the battery life of sensor nodes and IoT devices. This is particularly important in applications where replacing batteries frequently is impractical. For instance, in wildlife tracking, IoT

Table 1 Power Consumption for Each Component on the Sensor Node [20]

S. No.	Function	Device	Wake up time (In seconds)	Idle/ transmit current (mA)	Sleep Current (μA)
1.	RF module	XBee	15	29 / 120	2.5
2.	MCU	ATMega328	15.5	4.35	200
3.	Humidity	HIH5030	15	0.2	0
4.	Temperature	MCP9700	15	0.006	0
5.	CO_2	GC-0012	15	1.5	0
6.	CO	MiCS-5121WP	10.5	30.7	0
7.	LDO	MCP1700	10.5	0.0016	1.6
Total				65.7576 / 156.7576	204.1

* Where RF: Radio Frequency, MCU: Micro Controller Unit, LDO: Low Drop Out

Table 2 Power consumption for sensor node device [20]

Stage	Mode	Current (mA)	Power (mW)	Energy consumption (mJ)
1	Idle (0 to 10 seconds, 10.1 to 10.5 seconds)	65.8	217.14	2258.26
2	Transmit (10 to 10.1 seconds)	156.2	515.46	51.55
3	Idle (10.5 to 15 seconds)	35.1	115.83	521.24
4	Sleep (15 to 16 seconds)	4.3	14.19	14.19
5	Sleep (More than 16 seconds)	0.2	0.66	781.44

based GPS collars equipped with WSNs transmit animal location data while consuming minimal power. These devices can operate for months without battery replacements, ensuring long term monitoring of endangered species.

Despite its advantages, WSN technology faces several challenges that limit its ability to fully support IoT applications, especially those requiring high speed, low latency, and highly secure communication [16–19]. Due to the following reasons the WSNs sometimes may not provide adequate assistance:

1. Energy Constraints and Short Battery Life: WSN nodes typically rely on small batteries with limited power capacity, leading to frequent replacements or network failures, especially in long term IoT applications. Energy efficiency remains a significant challenge, particularly in large deployments. Tables 1 and 2 represent the power or current requirements for the sensor node [20]. For example, in healthcare applications, IoT based wearable devices that use WSNs require frequent battery recharging, limiting their practicality for continuous patient monitoring.
2. Limited Bandwidth and Data Transmission Range: Most WSN protocols, such as Zigbee, Bluetooth, and 6LoWPAN, offer only short range and low bandwidth communication, making them unsuitable for IoT applications requiring high speed, long distance data transmission. For instance, in autonomous vehicle networks, where real time, high speed communication is essential for vehicle-to-vehicle (i.e. V2V) and vehicle-to-infrastructure (i.e. V2I) interactions, WSNs fail to meet the required data transfer speeds and latency constraints.
3. High Latency in Data Processing: WSN nodes have limited processing power and memory, often resulting in delays in transmitting and analyzing data. This latency issue negatively impacts real time IoT applications that require immediate responses. For example, in industrial automation, robotic arms and automated conveyor belts depend on low latency communication to function efficiently. WSN based IoT systems with high latency may cause delays in production lines, reducing operational efficiency.
4. Vulnerability to Cybersecurity Attacks: Many low cost WSN nodes lack robust security mechanisms, making them a potential entry point for cyber threats such as data breaches, DoS attacks, and network hijacking. For instance, in smart grid systems, an insecure WSN based IoT network can be exploited by hackers to manipulate power distribution, leading to large scale energy disruptions and financial losses.

5. Difficulty in Large Scale Deployment and Maintenance: While WSNs enable scalability, managing thousands of sensor nodes across a large IoT deployment presents challenges in terms of network maintenance, firmware updates, and troubleshooting failures. For example, in traffic monitoring systems for smart cities, deploying and maintaining thousands of WSN enabled sensors on roads, intersections, and highways requires substantial resources, making it logistically complex and expensive.

While WSN technology offers numerous advantages for IoT applications, its widespread adoption is hindered by challenges such as limited energy availability, communication constraints, security vulnerabilities, and high operational costs. By integrating energy efficient solutions, advanced communication technologies, AI based processing, robust security mechanisms, and autonomous maintenance strategies, WSNs can be significantly improved, making them more reliable for large scale, real time, and mission critical IoT applications.

1.4 WSNs for energy efficient and secure communication in the IoT environment

WSNs provide energy efficient communication for IoT depends on the communication protocols, network topology, data transmission methods, and power optimization techniques used [3, 16–19]. WSN can support energy efficient communication in IoT if properly designed. However, standard WSN implementations may not always be efficient due to high power consumption in data transmission, routing overhead, and idle listening. The energy efficient communication matters in WSNs for IoT, due to, but not limited to:

- IoT applications require WSNs to operate for long periods with minimal power consumption.
- Many IoT devices are deployed in remote or harsh environments where frequent battery replacement is impractical.
- Data transmission over wireless links is one of the most power intensive processes.
- Prolonged network lifetime is essential for IoT applications like smart cities, industrial automation, and environmental monitoring.

Despite the advantages of WSNs for IoT application, several challenges remain. The following challenges highlight the need for further innovations in WSN for IoT domains.

- Scalability Issues: Large-scale IoT deployments require thousands of sensors, increasing energy demands.
- High Data Traffic: IoT applications generate massive real-time data, which burdens WSN energy consumption.
- Security & Encryption Overhead: Implementing security mechanisms consumes extra power.
- Environmental Factors: Harsh conditions can drain power (e.g., extreme temperatures reduce battery life).

The world's population is experiencing rapid growth, leading to increased demands from individuals [21]. The integration of advanced technologies such as IoT, artificial intelligence (i.e. AI), SDN, ML, computer vision, and DL into various aspects of daily life facilitates improved decision making [22–25]. These technologies also contribute to the automation (across various smart systems such as smart grids, smart water grids, smart cities, smart healthcare, smart parking, smart agriculture, and many more) of daily processes, delivering knowledge and services that enhance the quality of work in everyday life [26]. These smart systems are capable in sensing, collecting, transferring, and processing information by deploying a numerous sensors in physical environments [27]. Almost all physical gadgets today incorporate such sensor(s), continuously sending data about their surroundings and the condition of connected devices [28]. These sensors, utilizing wireless networks such as Zigbee, monitor environmental parameters, based on domain specific applications, such as temperature, humidity, moisture, and location in real time, aiding decision making [27]. However, these sensors face constraints related to memory, power/energy, and computing capabilities, leading to frequent battery depletion, impacting network lifetime [29]. Therefore, designing energy efficient mechanisms for these resource constrained sensor devices is crucial to ensure reliable and sustainable energy supply.

The availability of specific hardware devices for sensing particular parameters in smart systems raises concerns, as the demand for low cost smart devices often compromises security [30]. Various attacks, including side channel attacks and hardware trojans, are likely possible in hardware devices [22, 31]. Thus, ensuring secure communication among resource constrained sensor devices becomes challenging, necessitating the design of techniques for secure transmission in smart systems [30, 32]. Addressing issues such as energy [22, 33], security [30, 34–38], privacy [39–46], and heterogeneity (as

highlighted in table 7) in smart systems, including domains like smart health [38, 39, 47–53], smart grid [32, 42, 54–59], smart city [60], smart agriculture [31, 36, 61–64], and smart parking, is a primary focus of this paper (as presented in tables 11 and 12). Furthermore, the authors highlight the potential roles of advanced technologies such as SDN, ML, DL, 5G, D2D communication, cloud computing, computer vision, and edge computing in smart systems [36, 61, 63–73].

The influence of advanced technologies spreads throughout every aspect of life, including education, transportation, manufacturing, medicine, agriculture, engineering, and defense [36, 61]. The field of computer networks, as a discipline of engineering, has experienced significant impacts, with ML algorithms emerging as suitable tools for an evolving environment. ML algorithms facilitate the correlation of collected data that sensors may struggle to correlate independently, contributing to informed decision making [36, 61, 63–65]. However, the deployment of various sensors in smart systems, extracting real time parameters, leads to higher energy consumption, necessitating the development of intelligent network resource management mechanisms [74]. This includes aspects such as intelligent routing, energy efficiency, and intelligent security mechanisms. While advanced technologies, including IoT, contribute significantly to improving daily life, challenges such as hardware limitations, scalability, interoperability, energy management, security, cost, and data processing persist.

1.5 Organizational structure of present work

This paper is organized as follows (also shown in figure 6):

- Introduction: Section 1 introduces the study. This section mentions about IoT, sensor networks, and use of advanced technologies such as AI, SDN, ML, DL into various aspects of daily life in context of IoT environment. Later, it presents the proposed work of this paper. A list of abbreviations used in the text is also presented in table 3.
- Literature Survey: Section 2 describes several issues such as energy, security, privacy, and scalability and interoperability in several smart system domains such as smart grid systems, smart healthcare, smart agriculture, smart home/city etc.
- Major Takeaways: Then, section 3 presents several IoT frameworks and IoT architectures in the context of aforesaid issues. Afterwards, it also describes energy and security issues in smart systems. In addition to that, offline and online design paradigm is also mentioned in this section.
- Research Gaps: Several research gaps in literature survey are identified in section 4. These research gaps are: (a) security and privacy consideration into IoT frameworks and architectures, (b) security and privacy in a specific smart system, (c) heterogeneity in IoT network, (d) interoperability in IoT network, (e) lightweight cryptography, (f) offline and online design paradigm, (g) imbalance data communication in smart system, (h) energy hole problem, (i) lack of parameters for cluster head selection method, (j) use of advanced technologies, (k) cloud and edge computing, (l) lack of appropriate simulation environment, and (m) privacy preserving. The detailed discussion about these research gaps will be covered in section 4.
- Conclusion with Summary: Finally, the study is concluded in section 5.

1.6 Contribution of this study

The current study presents several key findings, summarized as follows:

- Lack of Standardized Framework and Architecture: The authors highlight that despite the presence of numerous frameworks and architectures for smart IoT systems, a standardized framework and architecture is still missing, often neglecting security and privacy aspects.
- Security and Privacy: Although security issues are addressed in different domains, the approach is not uniform, and this inconsistency similarly extends to privacy. As a result, there is an evident chance to develop solutions that integrate security and privacy considerations in domains that have not yet been fully addressed.
- Heterogeneity and Scalability: The analysis of heterogeneity, scalability, and interoperability challenges in IoT based systems, especially with regard to the variety of devices within the network, is lacking. This situation offers a chance to develop a scalable solution that can effectively manage the extensive range of IoT devices and the traffic they generate.

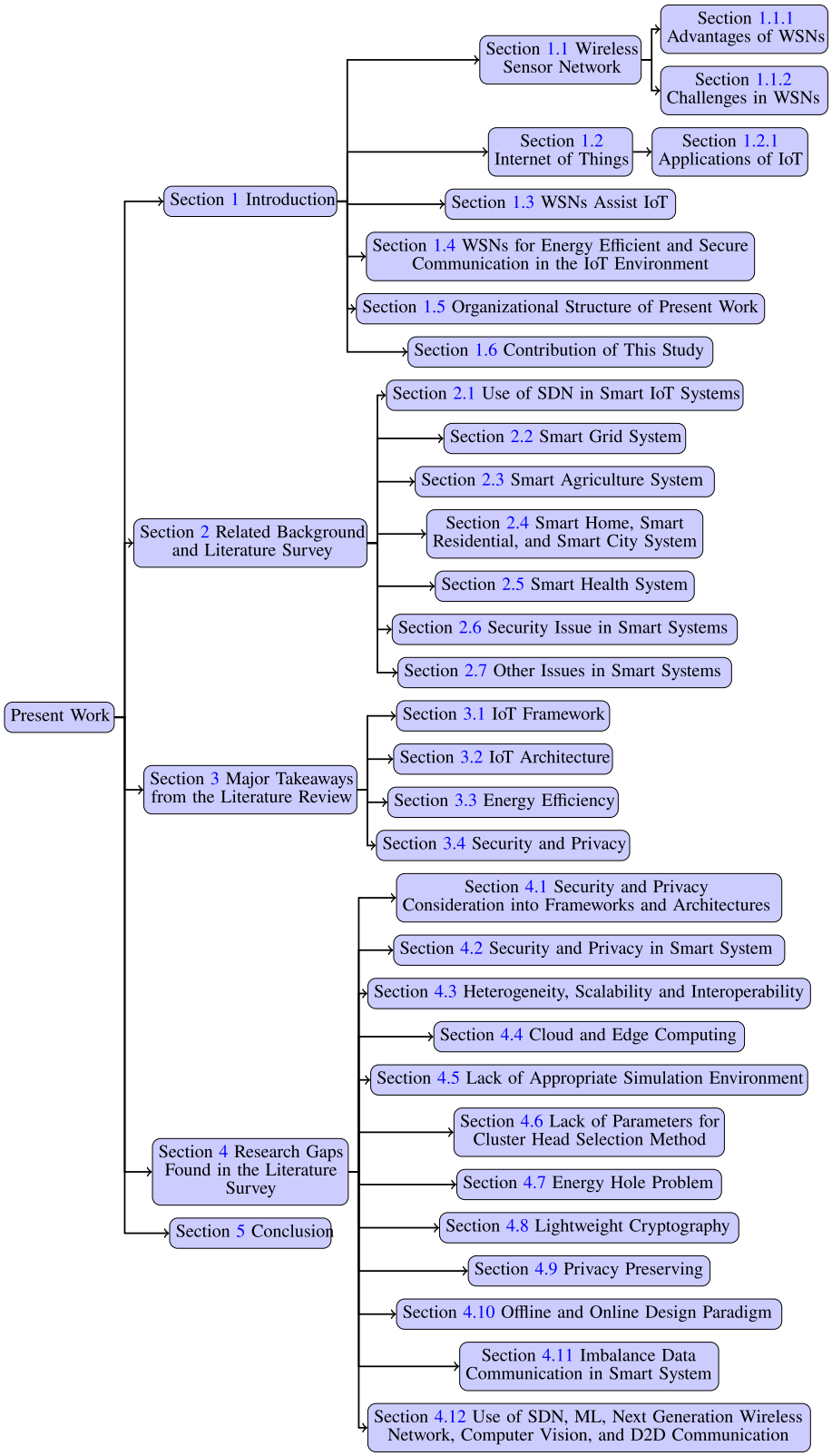


Fig. 6 Organizational chart of present work

- Network Edge: Data processing in the cloud consumes a significant amount of energy, primarily because of rising transmission costs and latency. IoT devices also require considerable energy. This situation presents an opportunity to explore data analysis within the network to optimize energy consumption and reduce latency.

Table 3 A list of the abbreviations used throughout in the text

S. No.	Abbreviation	Stands For
1.	D	Distance
2.	E	Energy
3.	I	Imbalance data communication
4.	L	Load
5.	5G	5^{th} Generation
6.	AI	Artificial intelligence
7.	De	Transmission delay
8.	DL	Deep learning
9.	ML	Machine learning
10.	ND	Node degree
11.	CHC	Cluster head count
12.	D2D	Device-to-device
13.	DoS	Denial of service
14.	IDS	Intrusion detection system
15.	IoT	Internet of things
16.	M2M	Machine-to-machine
17.	NFV	Network function virtualization
18.	QoS	Quality of service
19.	RAM	Random Access memory
20.	SDN	Software defined networking
21.	SNR	Signal-to-Noise Ratio
22.	UAV	Unmanned Aerial Vehicle
23.	ALAM	Anonymous Lightweight Authentication Method
24.	DDoS	Distributed Denial of Service
25.	IIoT	Industrial Internet of Things
26.	PISA	Protocol Independent Switch Architecture
27.	RFID	Radio Frequency Identification
28.	SLoc	Sink Node Location
29.	TDMA	Time Division Multiple Access
30.	LEACH	Low Energy Adaptive Clustering Hierarchy
31.	SCADA	Supervisory Control and Data Acquisition
32.	EEPROM	Electrically Erasable Programmable Read Only Memory
33.	LoRaWAN	Long Range Wide Area Network

- Multiple Parameters: The predominant focus of current research works on energy efficiency is on selecting cluster heads using criteria like distance, residual energy, and node degree. This narrow approach for selection of parameters highlights a gap and suggests the potential for developing an energy efficient mechanism in smart IoT systems by incorporating additional parameters, including load, cluster head count (i.e. CHC), delay, and signal-to-noise ratio (i.e. SNR), either individually or together.
- Lightweight Cryptosystems: Studies on privacy preservation and security enhancement frequently use public cryptosystems such as RSA and Elgamal. However, these cryptosystems are computationally demanding and consume considerable energy. As a result, there is a demand for lightweight cryptosystems to provide security and protect privacy in smart IoT networks.
- Offline and Online Design Paradigm: The authors identify that applying the offline and online design paradigm in smart IoT systems offers a promising approach to developing privacy preserving mechanisms that minimize energy consumption.
- Advanced Technologies: The current study also recognizes that advanced technologies like SDN, ML, 5G, D2D communication, big data, cloud computing, computer vision, and edge computing could significantly enhance the capabilities of smart systems.

2 Related background and literature survey

This section covers a comprehensive literature survey of various domains of smart systems such as smart healthcare, smart agriculture, smart grid, and smart home/city. For such smart systems, a detailed analysis of several critical aspects such as security and privacy concerns, scalability challenges, interoperability issues, and energy management considerations is undertaken in this present work. Through this survey, the efficacy of advanced technologies within the context of smart networks and systems is also assessed. Various application areas of IoT have been depicted in figure 5. Several of them will be discussed in subsequent sections or sub-sections.

2.1 Use of SDN in smart iot systems

This section starts with introductory information on SDN [75], and use of SDN in smart IoT systems. The SDN benefits legacy network topologies through dynamic flow control, network wide visibility, network programmability, and data plane simplification [75]. These features offer potential improvements to IoT networks, allowing for dynamic reconfiguration and adaptability to changing application behavior. SDN aids in optimizing network resources based on Quality of Service (i.e. QoS) requirements and virtualizing network functions to enhance processing capabilities. The OpenFlow protocol [76], originally developed for communication between network devices and SDN controllers, has limitations in supporting a fixed number of protocol header fields [77]. To address this, the Protocol Independent Switch Architecture (i.e. PISA) and the P4 language [78] allow for flexible and custom programming of switches, contributing to security and energy efficiency in IoT networks. As shown in table 4, the SDN may assist in security and energy efficiency for resource constrained IoT environment.

2.2 Smart grid system

The integration of SDN into smart grid systems holds significant potential for enhancing efficiency and resilience. In the context of smart grids, SDN is employed for monitoring and controlling communication networks. Leveraging the features of SDN proves advantageous in seamlessly integrating diverse smart grid protocols and standards. These protocols and standards govern various communication systems, traffic flow organization, and specific QoS requirements within the smart grid domain. Addressing the network requirements of a smart power distribution grid system, the a SDN based solution is proposed [40]. Stability and efficiency are crucial for the Supervisory Control and Data Acquisition (i.e. SCADA) network within a smart grid, especially considering vulnerabilities to cyber threats. By incorporating advanced technologies into the SCADA network, improved communication management and the formulation of innovative grid control algorithms are facilitated [59].

In another context, an architecture is presented for the integration of plug-in electric vehicles into a smart grid [79]. This architecture introduces automated and flexible operations at each control level, ultimately accelerating service innovation within the plug-in electric vehicles integrated smart grid. Additionally, a real time dynamic pricing model for electric vehicle charging and discharging services, coupled with building energy management, is proposed in article [80]. This model adopts a decentralized cloud computing architecture to mitigate peak demand effectively.

A study outlined in [81] employs real time monitoring techniques to establish a platform based on Industrial Internet of Things (i.e. IIoT) for ensuring resiliency in smart grid networks. The platform reacts promptly to rectify issues, thereby enhancing the reliability of smart grid networks. Furthermore, a detailed survey of various routing protocols for Long Range Wide Area Network (i.e. LoRaWAN) multi-hop networks is provided by study [58]. The researchers designed a routing system, wherein a specific node relays data from leakage detection nodes, facilitating efficient peer-to-peer communication between end devices in the smart water grid.

The utilization of SDN enables the creation of a durable, robust, and flexible communication framework for smart grids [82]. IIoT finds application in various sectors, including smart grid energy management, transportation, manufacturing, and healthcare. Article [35] introduces an SDN enabled secure communication architecture for IIoT, emphasizing security in the context of this evolving technology. Study [42] suggests a privacy preserving framework for the smart grid to enhance privacy while minimizing network cost. Additionally, the applications of ML technologies for

Table 4 Various Features of SDN and their Potential Contribution to Security and Energy Efficiency in IoT Networks

S. No.	SDN feature	Feature description	Benefit to security	Benefit to energy
1.	Dynamic Flow Control (Through Real Time Network Measurements)	SDN can dynamically control network flows (e.g., reroute, forward, and drop)	Control dangerous or harmful network flows/packets dynamically, and distinguish harmful network flows from benign ones	For energy efficiency in SDN, flow management and load balancing techniques can be used to mark certain network devices to be switched off or to work at reduced energy levels for certain durations
2.	Network Wide Visibility with Centralized Control	A centralized server may monitor and handle all network status and flow information	Monitor the whole network for security services in a centralized manner, detecting network anomalies easily and effectively	A SDN controller may make choices based on the system's traffic load, enabling effective resource usage. Nodes with no traffic can be put to sleep, while nodes with low traffic can be diverted to a few active networks to offer the service
3.	Network Programmability	Network functionalities can be programmed by using SDN i.e. partially in OpenFlow enabled networks or fully in P4-enabled switches	Build network security services quickly and efficiently, opening the door to building complicated network security services	Saving energy in the network may be accomplished by programming the network based on traffic conditions
4.	Data Plane Simplification	SDN simplifies the data plane by eliminating complex control plane logic	Change the data plane as a form of security device by adding additional modules	Using dataplane supported frameworks like In-band network telemetry, the number of messages required for telemetry can be reduced

data analysis in smart grid system are explored, with a specific focus on privacy concerns related to user electricity usage data clustering [57].

A literature review in study [54] addresses authentication, authorization, and accountability in smart grid systems, proposing a system that augments existing frameworks such as [82] with a security component based on the *IEEE*802.1*X* standard. Furthermore, study [56] conducts a comprehensive assessment of security and privacy measures in SDN based smart grid communication, along with a detailed discussion of SDN based smart grid communication routing systems. Recognizing the challenges associated with a swift transition to purely SDN enabled devices in a smart grid, researchers in work [59] suggest a framework for constructing a hybrid network that incorporates both traditional forwarding devices and programmable SDN enabled switches. A generic overview of smart grid system is shown in figure 7.

2.3 Smart agriculture system

As mentioned earlier, the world's population is experiencing rapid growth, resulting in an increased demand for food production. Smart agriculture heavily relies on automation machinery, demanding a substantial number of electronic components that consume significant power. To address this demand, advanced technologies like IoT, AI, and ML have been integrated into agriculture, empowering farmers to make informed decisions. Smart agriculture involves the deployment of a massive number of sensors in farms, utilizing wireless networks to collect diverse parameters for real time monitoring and enhanced crop production [31, 36, 61]. The extraction of various parameters in real time increases communication requirements, leading to more energy consumption. However, as previously stated, these sensors face constraints in terms of memory, power/energy, and computing capabilities. The frequent depletion of batteries, due to high communication activity, poses a significant challenge, leading to sensor stops and a reduced network lifespan.

A smart IoT system employs sensor data collection, transferring the data to the cloud for processing and analysis. In the domain of smart farming, Information and Communication Technologies, IoT, cloud and edge computing, robotics, SDN, and AI play crucial roles. The integration of IoT in agriculture empowers farmers to make informed decisions, potentially automating farming processes to enhance production, quality, and profitability [61]. A rapid transition from traditional agriculture to smart management, facilitated by various IoT firms, is evident as farmers adopt advanced technologies to optimize yields and meet growing demand [63]. The substantial volume of data generated is processed and analyzed in the cloud, providing valuable insights and critical information to agricultural businesses. Edge computing has mitigated the costs associated with data transmission, processing, and storage from smart IoT systems in the cloud. Edge computing involves processing data at the network's edge before transmission to the cloud, resulting in quicker response times and ensuring continued service provision even in the event of a link failure between the IoT device and the cloud. Study [65] proposes a data flow management technique in SDN and NFV using an Edge and IoT architecture. Another study [84] successfully develops a wireless communication control system within the farm's range, receiving sensor data as inputs and generating output based on predefined criteria. The study finds that sensor testing values vary with environmental conditions, time of day, and test location, while also noting low development costs and labor requirements, making it suitable for many farms.

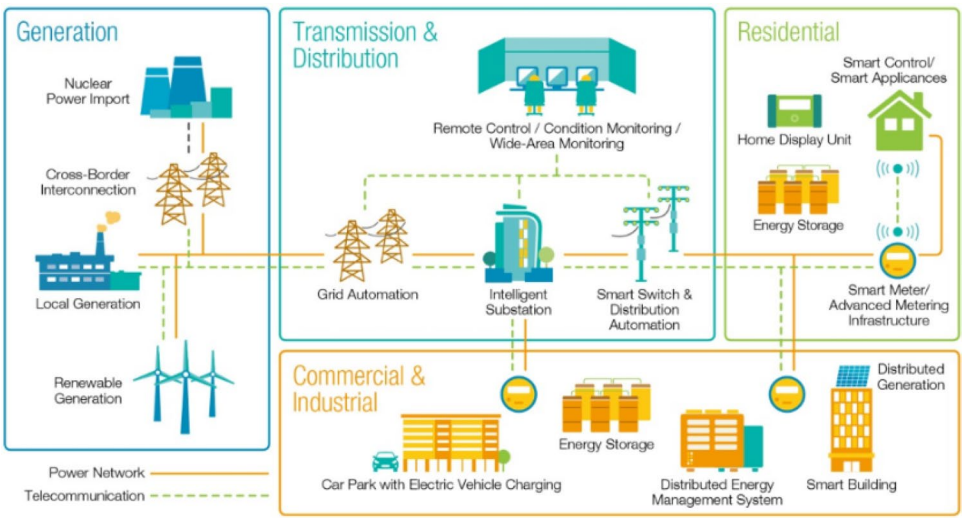


Fig. 7 A generic overview of smart grid system [83]

A study [64] introduces an framework that provides a consistent set of perspectives for modeling IoT based systems in the agriculture sector. In another paper [36], an architecture integrates blockchain technology, fog computing, and SDN. Based on the cyber physical system IoT and SDN, a hypothetical network architecture for urban farming and precision agriculture in smart cities is presented [85]. Article [61] conducts a comprehensive review of advanced technologies for smart agriculture, starting with an analysis of past research and identifying upcoming technologies such as wireless technologies, open source IoT platforms, Unmanned Aerial Vehicles (i.e. UAVs), cloud computing, edge computing, fog computing, SDN, NFV, and middleware platforms for agriculture. An analysis in article [63] highlights the transformative impact of multiple technologies, including ML, AI, edge computing, and SDN, on smart agriculture, emphasizing the importance of interdisciplinary approaches for its future. The study develops a multidisciplinary architecture for efficient and cost effective agricultural solutions, providing a list of industrial solutions for various aspects of farm management and underlying targeted technologies. Figure 8 demonstrates a IoT based smart agriculture management system.

2.4 Smart home, smart residential, and smart city system

In study [87], the authors introduced a smart house, centered around a controller capable of communicating with various smart devices and featuring open APIs for third party service integration. Such smart houses proactively address potential customer needs, offering a universal platform for device control. The authors demonstrated a wearable wireless gait sensor device designed for home monitoring of gait disabled patient's specific symptoms [88]. This system identifies abnormal gait, prevalent in post-stroke patients, in a robust and reliable manner. Also, this proposed system aims to provide virtual gaming treatment to post-stroke patients, aiding in their recovery from mobility issues. Integrating NFV and SDN with televisions at home holds the potential to provide customers with smart TV services while enhancing their overall quality of experience [89]. A study [89] focused on a follow-me-service in home networks, allowing users to use their smartphones to select media content and play it on the nearest TV set, continuing seamlessly to other TV sets while moving around their home.

In study [90], a detailed analysis of a secure communication infrastructure at various scales was conducted. The authors proposed a methodology for safety monitoring and management in dynamic spatial contexts, such as ports, by combining IoT and multi-agent geo-simulation techniques [91]. A SDN based solution adapts the number of bytes in packets to variations in home network consumption, ensuring the length of packets generated by connected devices remains unchanged [40]. The privacy improvement was quantified using metrics like accuracy, recall, and F-1 score through various supervised learning algorithms. Figure 9 shows a basic smart home system, whereas figure 10 presents an intelligent transportation system in smart city system.

2.5 Smart health system

Smart healthcare networks have emerged as a transformative healthcare system capable of significantly improving the quality of life for individuals. This innovative approach offers patients more efficient and high quality medical care, and the integration of the advanced technologies holds the potential to enhance user experiences. Smart healthcare

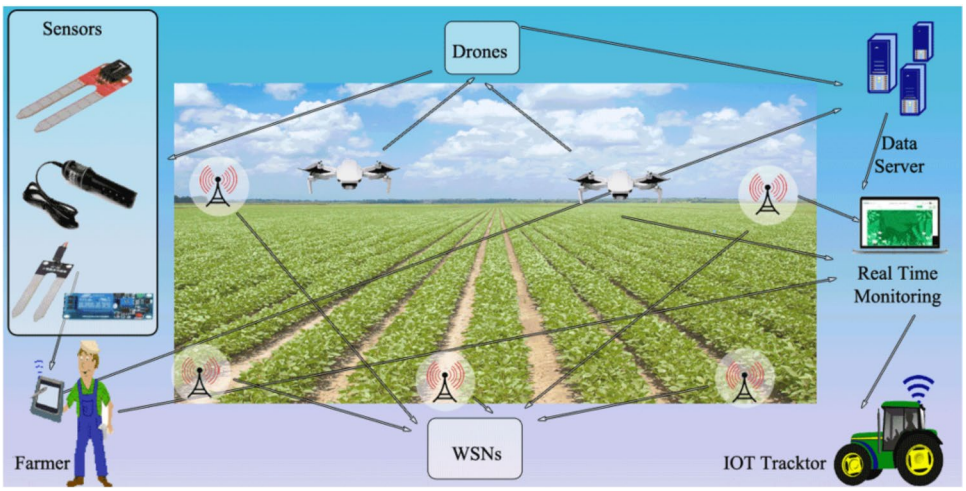


Fig. 8 Overview of IoT based smart agriculture system [86]

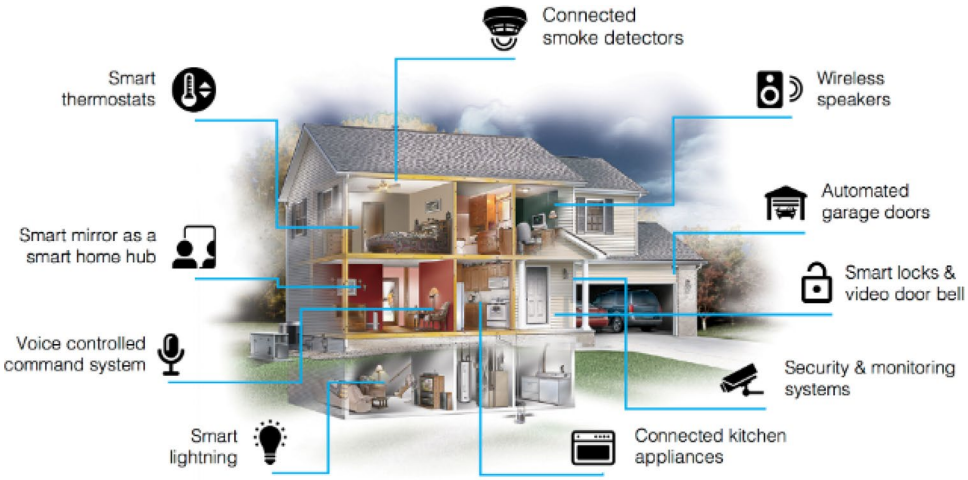


Fig. 9 Overview of smart home system [92]

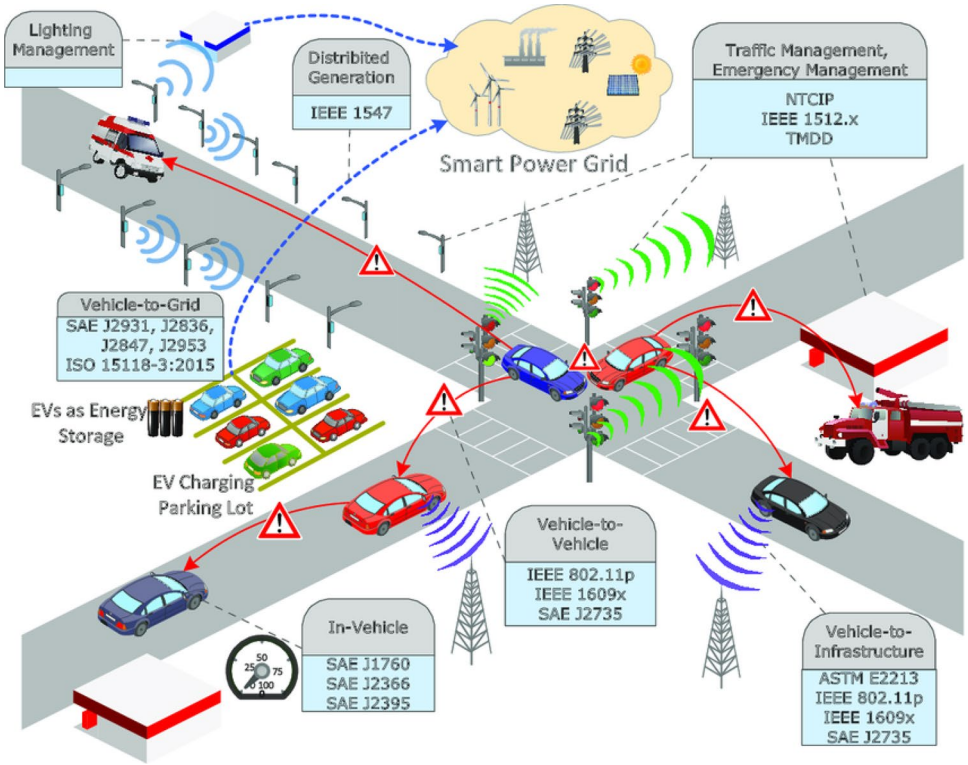


Fig. 10 Intelligent transportation in smart city [93]

initiatives have been initiated in various countries, with ongoing pilot projects in healthcare organizations. Within the smart healthcare system, IoT devices play a pivotal role in collecting diverse personal health related data. The massive number of sensors and wireless smartphone communication has become integral to daily living. To address the diverse requirements of widespread healthcare applications, the authors proposed an architecture encompassing end user devices, edge servers, and cloud servers [47]. SDN dynamically manages this architecture, enforcing network regulations and orchestrating healthcare services. A wireless body area network acquires information from body sensors, transmitting aggregated data to edge or cloud servers for additional processing and decision making due to the constrained nature of the deployed sensors. In article [51], a personal digital assistant is configured as an SDN switch, demonstrated through Mininet, showcasing the feasibility of this approach in wireless body area networks with low deployment complexity and network overhead, effectively managing connected devices and their connections.

Cloud computing is leveraged for on-demand processing of IoT data [52]. In a mobile healthcare social network, the signature based symptom matching algorithms are devised to offer both coarse grained and fine grained symptom

matching, ensuring privacy without reliance on a third party [39]. In an edge computing healthcare system [38], edge servers authenticate IoT devices using a lightweight authentication technique. Following authentication, these devices collect patient data, transmitting it to edge servers for storage, processing, and analysis. The SDN controller links edge servers to load balancing, network optimization, and efficient resource utilization in the healthcare system. An intrusion detection framework proposed in work [94] combines host and network based techniques for effective IoT intrusion detection, adopting a collaborative approach while minimizing performance overhead to conserve IoT device resources. Health-Flow, introduced in article [50], employs ML to identify flow criticality and mobile device locations, enhancing the efficiency of a smart healthcare network. Edge computing is proposed as a solution to computational and processing challenges, providing cost effective solutions and improving the connectivity and processing performance of IoT devices in a healthcare system, leading to low latency data services [60]. In a work [95], an integrated public IoT framework for smart governance is proposed, combining IoT concepts with crucial business related or value added components beyond the predominant technological viewpoint. Additionally, an article [96] introduces a configuration framework for constrained IoT devices based on open standards, specifically the Constrained Application Protocol. The smart healthcare management system is mentioned in figure 11.

2.6 Security issues in smart systems

Since certain security and privacy aspects have already been discussed in the previous sections, this section addresses several additional security and privacy related risks, as highlighted in figure 12. Data retrieval, analysis, and transmission are routine processes that demand substantial effort and pose challenges in maintenance due to the sheer volume of data generated [22]. The lack of a structured framework for data handling in sensor or IoT devices makes them susceptible to potential security breaches, allowing attackers to gain unauthorized access [36]. The chaotic accumulation of data without systematic or scientific methodologies increases the vulnerability of the system [37]. To effectively manage the vast and scattered data, SDN is integrated into IoT applications, employing a central controller for network design and maintenance [36, 37]. SDN enables dynamic adjustments to data behavior and operational procedures programmatically, preserving the underlying physical architecture [75].

Numerous threats exist that have the capacity to disrupt the entire system, with some posing risks of complete system failure [56]. Privacy concerns arise when a third party gains concealed access to the communication between two clients [42]. The security challenges of resource constrained IoT devices, identity theft attacks, and insider

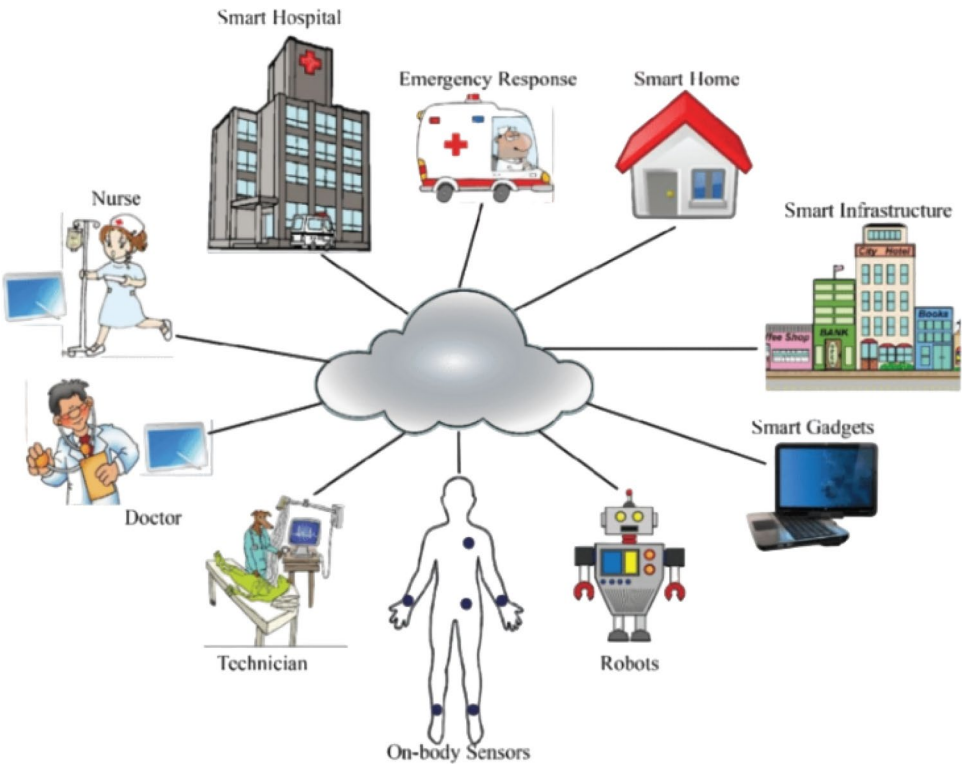


Fig. 11 Basic overview of smart healthcare system [97]

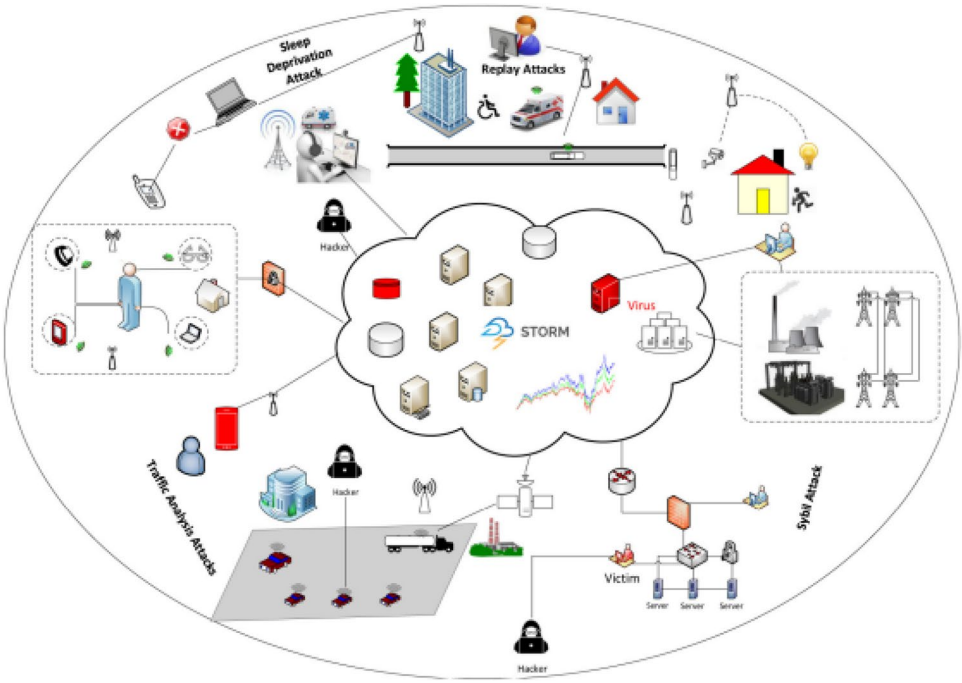


Fig. 12 Various security issues in smart IoT environments [98]

threats in smart healthcare systems are addressed through the design of a security enforcement architecture for intelligent healthcare data sharing systems [49]. Denial of service (i.e. DoS) attacks have the potential to render services inoperable for extended duration, posing an inherent challenge in IoT networks [99]. SDN is employed to address these issues swiftly, as it can promptly identify abnormalities and serve as a primary defense against attackers [22]. In pursuit of cyber attack resilience, the authors of article [100] propose a "self-healing" phasor measurement unit network leveraging the dynamic and programmable configuration attributes. Post cyber attack, network switches are reconfigured to isolate compromised phasor measurement units, preventing further spread of the attack. Simultaneously, disconnected but uncompromised phasor measurement units are reconnected to the network, facilitating "self-healing" and restoring observability to the power system. Article [60] investigates various security flaws, attack channels, and potential solutions. BlockSDN [60] is developed to mitigate multiple vulnerabilities, addressing scenarios such as a malware infected switch at the data plane and a distributed DoS (i.e. DDoS) attack at the control plane. Additionally, article [32] delves into the vulnerability of battery energy storage systems in smart distribution networks to fake data injection attacks, providing a foundation for further research into attack techniques against these systems and offering a theoretical guide for defense development.

Even in the absence of a direct connection between IoT devices and users, these devices often learn usage patterns to deliver services and convenience. While these IoT devices streamline daily services, they also pose potential threats to privacy. Traffic pattern analysis of frequently used devices may reveal sensitive information, such as a person's presence at home. The analysis of connected device's traffic in a home environment raises privacy concerns [40]. A study [101] introduces a privacy preserving security architecture for smart homes, incorporating an anonymous lightweight authentication method (i.e. ALAM). The ALAM protocol, as authors claimed, withstands security threats while ensuring secure mutual authentication and user anonymity. However, a study [102] challenges the claim that the ALAM protocol provides user anonymity and mutual authentication. Many IoT devices lack essential security measures, leading researchers in study [103] to focus on detecting horizontal port scans in residential networks. They demonstrated a firewall technology capable of detecting such scans, utilizing FleXight as an information channel between the SDN controller and data route components.

In a smart network, the number of insecure and portable devices is rapidly increasing, posing cyber security challenges. Existing solutions face inefficiencies due to storage limitations, high energy consumption, underutilized

resources, significant latency, and a single point of failure [22]. Security issues in smart cities, such as threatening data and service security and availability through traffic flooding, prompted the development of a DDoS attack defense approach based on traffic classification [99].

2.7 Other issues in smart systems

In this section, the critical aspects of energy management, scalability/interoperability, edge computing, and cloud computing challenges within IoT networks are delved. Given that IoT devices predominantly rely on battery sources, energy efficiency emerges as a pivotal concern in IoT deployment, necessitating strategies to extend the overall network lifespan. Various energy efficient techniques are explored, as discussed in work [29], which covers duty cycle management, wake-up radios, sleep/wake cycles, and topology control, each with its distinctive set of limitations and advantages. A work [104] undertakes a comparative analysis of popular options in adopting new energy platforms, introducing a comprehensive evaluation framework for IoT technology adoption.

Edge computing serves as a paradigm that offloads computation from cloud servers to systems at the network edge, yielding benefits such as reduced latency, enhanced security, and privacy protection. An article [33] conduct a review on energy aware edge computing, emphasizing key concerns and directions encompassing architecture, operating systems, middleware, application services, and offloading. In addressing the dual challenge of quick charging station selection and electric vehicle route planning, a study [105] employs SDN and vehicular edge computing approaches. The objective is to minimize overall customer expenditure while considering time, charge fees, charging availability, and energy price variations. The study introduces a deep reinforcement learning based technique for optimal charging scheduling of low battery electric vehicles and a robust charging strategy based on incremental updates to enhance the electric vehicle driver's user experience.

For intelligent decision making in electric vehicle charging and discharging, a work [106] proposes an edge and cloud based system where both types of devices collaborate, ensuring a balanced demand-supply scenario. The authors present a blockchain and SDN based architecture for smart cities in [22], where SDN monitors and manages IoT device activities, blockchain provides security and privacy against cyber attacks, and NFV optimizes energy usage, load balancing, and network longevity. An empirical probability based control mechanism is developed in [107] to reduce network load and effectively manage bandwidth, optimizing data transfer using SDN. This approach minimizes transmission delays, contributing to swift transit of dimensionally reduced data between nodes.

Addressing interoperability and energy efficiency gaps, a detailed IoT taxonomy is presented in [27], covering all aspects of IoT. The study [27] identified industrial integration and technological barriers, evaluating the impact of different energy harvesters linked to IoT devices. In addition to that, the research gaps at industrial and technological levels were also highlighted, emphasizing the need to address heterogeneity and energy use underlying IoT devices [27].

Several previous survey works and case studies are compared with the present survey work, as shown in table 5. These previous survey works are lacking to address all the problems or issues (explained as research gaps in the section 4) for various IoT applications, and also lacking while suggesting the solutions for these issues. An energy inefficient IoT system leads to frequent battery depletion, ultimately reducing the overall network lifetime. Similarly, an insecure system risks unauthorized data disclosure, compromising sensitive information. To address security concerns in resource constrained IoT nodes, lightweight security algorithms can be employed to provide adequate security without significantly impacting performance. Scalability is another crucial factor in IoT systems. If a system lacks scalability, it will fail to support a large number of sensor nodes within a network, limiting its applicability in extensive deployments. Additionally, heterogeneity and interoperability play a significant role in ensuring that nodes with different configurations, manufactured by various vendors, can effectively communicate and collaborate. To optimize energy consumption, several operations can be executed during the offline phase when a node is idle. This approach helps conserve energy and extend the network's operational life. Furthermore, data collection by a sink node from multiple member nodes simultaneously is a challenging task, requiring efficient communication and coordination mechanisms. The integration of advanced technologies such as ML, DL, Computer Vision, D2D communication, 5G networks, SDN, AI, and edge and cloud computing can significantly enhance the performance of WSN based resource constrained IoT environments. These technologies contribute to improving efficiency, security, scalability, and overall network functionality.

Table 5 Comparison of Present survey work with previous survey works

S. No.	Reference No.	Description
1.	[29]	• Explored various energy efficient techniques which covers duty cycle management, wake-up radios, sleep/wake cycles and topology control, each with its distinctive set of limitations and advantages · Energy Consumption: ✓ · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: ☒
2.	[33]	· Conducted a review on energy aware edge computing, emphasizing key concerns and directions encompassing architecture, operating systems, middleware, application services, and offloading · Energy Consumption: ✓ · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: ✓ · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: Edge Computing (✓)
3.	[56]	· Studied a comprehensive assessment of security and privacy measures in SDN based smart grid communication, along with a detailed discussion of SDN based smart grid communication routing systems · Energy Consumption: × · Security, and Privacy: ✓ · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: SDN (✓)
4.	[58]	· Explored the utilization of edge computing and cloud computing to facilitate swift data processing and also surveyed various routing protocols for LoRaWAN multi-hop communication networks · Energy Consumption: × · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: ✓ · Imbalance Data Communication: × · Use of Advanced Technologies: Edge and Cloud Computing (✓)
5.	[61]	· Presented a review of advanced technologies for smart agriculture by identifying technologies such as wireless technologies, open source IoT platforms, UAV, cloud computing, edge computing, fog computing, SDN, NFV, and middleware platforms for agriculture · Energy Consumption: × · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: ML, DL, 5G, SDN, NFV, UAV, Cloud, and Edge (✓)

Discover Internet of Things (2025) 5:56 | https://doi.org/10.1007/s43926-025-00152-2

Table 5 (continued)

S. No.	Reference No.	Description
6.	[63]	· Highlighted the transformative impact of multiple technologies, including ML, AI, edge computing, and SDN, on smart agriculture, emphasizing the importance of interdisciplinary approaches for its future · This study also developed a multidisciplinary architecture for efficient and cost effective agricultural solutions, providing a list of industrial solutions for various aspects of farm management and underlying targeted technologies · Energy Consumption: × · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: AI, ML, DL, SDN, Edge Computing (✓)
7.	[64]	· Introduced an framework that provides a consistent set of perspectives for modeling IoT based systems in the agriculture sector · Energy Optimization: × · Security, and Privacy: ✓ · Heterogeneity, Scalability, and Interoperability: ✓ · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: ☒
8.	[90]	· Conducted a detailed analysis of SDN's main functions in terms of a secure communication infrastructure at various scales · Energy Optimization: × · Security, and Privacy: ✓ · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: ☒
9.	[104]	· Highlighted a comparative analysis of popular options in adopting new energy platforms, introducing a comprehensive evaluation framework for IoT technology adoption · Energy Optimization: ✓ · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: ☒

Table 5 (continued)

S. No.	Reference No.	Description
10.	[108]	· Explored the differential evolution, a ML based approach, for routing optimization, overcoming redundancy, and addressing the energy hole problem · Energy Optimization: ✓ · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: ☒
11.	[109]	· By integrating the ML techniques, a run time architecture evaluation method was proposed for IoT, addressing challenges such as unpredictability, scalability, and performance · Energy Optimization: ✓ · Security, and Privacy: × · Heterogeneity, Scalability, and Interoperability: × · Lightweight Cryptography: × · Offline and Online Design Paradigm: × · Imbalance Data Communication: × · Use of Advanced Technologies: ☒
12.	Present Work	· The authors identify the absence of a standard framework and architecture for smart IoT systems, emphasizing the need for considerations related to security, privacy, and energy optimization (as mentioned in tables 6 and 7) · Furthermore, the authors also highlight the potential roles of advanced technologies such as SDN, ML, 5G, D2D communication, cloud computing, computer vision, and edge computing in smart systems · Energy Optimization: ✓ · Security, and Privacy: ✓ · Heterogeneity, Scalability, and Interoperability: ✓ · Energy Hole Problem: ✓ · Lightweight Cryptography: ✓ · Offline and Online Design Paradigm: ✓ · Imbalance Data Communication: ✓ · Use of Advanced Technologies: ✓

* Where ✓: Considered, ×: Not Considered, ☒: None Considered, ✓: All Considered

Discover Internet of Things (2025) 5:56 | https://doi.org/10.1007/s43926-025-00152-2

Table 6 Analysis of various IoT frameworks in terms of security and privacy, scalability, interoperability, and energy optimization

S. No.	Reference No.	Domain	Purpose	Security and Privacy	Scalability and Interoperability	Energy Optimization
1.	[30]	Manufacturing systems	Define cyber physical microservice and corresponding framework	×	✓	×
2.	[37]	Ad hoc vehicular network	Vehicular traffic management	×	×	✓
3.	[53]	Smart devices	Interaction with the cloud and connectivity between smart devices	✓	✓	✓
4.	[64]	Food and farming	Advanced and remote operation control	✓	✓	×
5.	[91]	Healthcare, Peer-to-peer	Provide complex security services	✓	×	×
6.	[94]	Healthcare, defense, satellite communications	Maintaining confidentiality during data communication	✓	×	×
7.	[95]	Healthcare	Analyze patient's health records	✓	×	×
8.	[96]	Healthcare, wearables, connected vehicles, object tracking	Implement a low power hybrid wired/ wireless sensor	✓	×	✓
9.	[110]	Multimedia	Multimedia service optimization	✓	×	✓
10.	[111]	IoT devices	Detection of zero-day DoS attacks	✓	×	×
11.	[112]	IIoT	Industry IoT Implementation	×	×	×
12.	[113]	IoT applications	Rapid implementation of IoT applications	✓	×	✓
13.	[114]	Constrained IoT Devices	Intrusion detection at the device and edge router levels	✓	✓	✓
14.	[115]	Transport and logistics	A virtual replication of the real-world to evaluate safety situations	✓	✓	×
15.	[116]	IoT forensic	Investigating IoT related crimes	✓	✓	×
16.	[117]	Educational Institutes	Prediction of student's future learning behavior	✓	✓	×
17.	[118]	Govt organizations	Improving public IoT services	×	✓	×
18.	[119]	Smart homes	Control and manage household gadgets	✓	✓	×
19.	[120]	Distributed applications	Allows devices to communicate with one another	✓	✓	×
20.	[121]	IoT gateways and devices	Interaction between the local and public networks	✓	✓	×
21.	[122]	Constrained IoT devices	Configure heterogeneous constrained devices	×	✓	✓
22.	[123]	Social IoT	Building a distributed programming ecosystem for social IoT	×	✓	×
23.	[124]	Sensor networks	Sensor software reusability, adaptability, and maintainability	✓	✓	×
24.	[125]	Smart applications	Using a smartphone, dynamically update IoT devices	×	✓	×

* Where ✓: Considered, ×: Not Considered

3 Major takeaways from the literature review

This section involves an in-depth analysis of multiple research studies that discuss diverse architectures and frameworks proposed by various authors within the smart IoT application domains. The principal observations and inferences are consolidated comprehensively. While the IoT has a substantial influence on smart systems, it is imperative to acknowledge and scrutinize certain pivotal takeaways alongside research gaps that necessitate attention. The major takeaways, inferred from an extensive literature review, will be systematically explained in the subsequent section, wherein due consideration will be given to the research gaps for further analysis in section 4.

3.1 IoT framework

IoT frameworks play a pivotal role in facilitating the development, deployment, and management of IoT applications. Table 6 provides a comparative analysis of security, scalability/interoperability, and energy efficiency factors across diverse IoT frameworks, as published by different researchers and/or industries. In this section, these frameworks may also consist of various other IoT applications and domains not defined in the section 2. Within the tabulated data, it is worth paying attention that out of the total 24 frameworks, 17 (i.e. nearly 71%) do not incorporate energy optimization, 9 (i.e. more than 37%) do not incorporate scalability/interoperability, and 7 (i.e. approximate 29%) overlook security and privacy considerations.

3.2 IoT architecture

In 2012, the European Telecommunications Standards Institute introduced a machine-to-machine IoT architecture to establish standardization for machine communication. Subsequently, in 2014, the IoT World Forum announced a seven layer reference architecture for IoT, drawing inspiration from the seven layer reference architecture of the OSI model. Following these developments, numerous researchers have proposed variations such as five layer, four layer, and three layer IoT architectures, derived from the foundational seven layer IoT architecture. Hence, there is a lack of standardized IoT architecture. Table 7 provides a comparative assessment of energy efficiency and scalability/interoperability across several IoT architectures proposed by diverse researchers. These architectures may also consist of various other IoT applications and domains not defined in the section 2. From this table, it is observed that among the 14 architectures, 6 (i.e. around 43%) do not incorporate scalability/interoperability whereas 7 (i.e. 50%) overlook energy optimization.

Table 7 Comparative Analysis of energy efficiency, scalability, and interoperability at the architectural level in IoT networks

S. No.	Reference No.	Domain	Architecture	Energy efficiency	Scalability and interoperability
1.	[48]	Healthcare monitoring	3 Layer	✓	×
2.	[64]	Agricultural IoT	4 layer	×	✓
3.	[109]	Traffic monitoring	3 Layer	✓	×
4.	[126]	IIoT for pollution control	5 layer	✓	×
5.	[127]	Environmental monitoring and forecasting	3 layer	✓	✓
6.	[128]	Enterprise IoT	5 Layer	×	✓
7.	[129]	Decentralized efficient resource utilization	3 Layer	✓	×
8.	[130]	IDS	3 Layer	×	×
9.	[131]	Smart city	4 Layer	×	✓
10.	[132]	Machine to machine interaction	3 Layer	×	✓
11.	[133]	Cloud and edge applications	3 Layer	✓	×
12.	[134]	Fog application	3 Layer	✓	✓
13.	[135]	Vehicular monitoring system	3 Layer	×	✓
14.	[136]	oneM2M	3 Layer	×	✓

* Where ✓: Considered, ×: Not Considered

Table 8 Summary of parameters for cluster head selection methods

S. No.	Reference No.	Parameters for cluster head selection methods								
		D	E	ND	CHC	De	L	SNR	SLoc	I
1.	[22]	✓	✓	×	×	×	×	×	×	×
2.	[139]	✓	✓	×	×	×	×	×	×	×
3.	[140]	✓	✓	×	×	×	×	×	×	×
4.	[141]	✓	✓	×	×	×	×	×	×	×
5.	[142]	✓	✓	✓	×	×	×	×	×	×
6.	[143]	✓	✓	×	×	×	×	×	✓	×
7.	[144]	✓	✓	✓	×	×	×	×	×	×
8.	[145]	✓	✓	✓	×	×	×	×	×	×
9.	[146]	✓	✓	✓	×	×	×	×	✓	×
10.	[147]	✓	✓	✓	×	×	×	×	✓	×

D Distance, *E* Energy, *ND* Node Degree, *CHC* Cluster Head Count, *De* Transmission Delay, *L* Load, *I* Imbalance Data Communications, *SLoc* Sink Node Location, *SNR* Signal to Noise Ratio. ✓: Considered, ×: Not Considered

3.3 Energy efficiency

The authors have observed a common practice in the IoT environment where, aiming to conserve energy or minimize power consumption, sensors sometimes occasionally opt not to transmit data directly to processing units or servers [21, 28, 74, 137, 138]. Instead, they transmit the data to intermediary IoT devices, which, in turn, relay the information to processing units. The literature on computing energy efficient paths often neglects to account for the possibility of intermediate forwarding devices experiencing failures due to battery depletion [22, 137]. In the context of IoT, data generated by IoT devices undergoes processing on the cloud, a pivotal step for decision making and historical analysis. It is imperative to recognize that the energy consumption of data processing in the cloud escalates with increasing transmission costs and latency. Additionally, energy intensive operations such as data collisions, re-transmission, sensing, transmitting, and receiving significantly contribute to the overall energy expenditure of IoT devices [27]. Among common operations like data gathering, data collection, and data processing, the latter involves processing units or servers to derive decisions and conduct analyses. Consequently, quick and speedy data processing is essential for making accurate decisions, analyses, or observations. Researchers have explored the utilization of edge computing and cloud computing to facilitate swift data processing, as evidenced by studies [22, 36, 58, 106].

Managing energy efficiency and adapting to changing link conditions are vital considerations for mechanisms governing data forwarding between sensor nodes. To conserve energy and extend the sensor network's lifetime, a clustering technique [21, 22, 137, 139–147] has proven effective. In clustering technique, a designated cluster head dynamically leads a group of member nodes, optimizing intra-cluster and inter-cluster communications. However, clustering near the base station can lead to an energy hole or hot spot problem due to increased communication and energy consumption. The unequal clustering mechanism aims to address this issue by minimizing cluster size near the base station, thereby balancing communication overhead.

The Low Energy Adaptive Clustering Hierarchy (i.e LEACH) approach [148, 149] stands out as a well known clustering strategy designed to reduce energy consumption. It operates in rounds, involving setup and steady state phases, where cluster heads communicate with sensor nodes, establish Time Division Multiple Access (i.e. TDMA) sessions, and aggregate data for transmission to the base station in a single hop [150]. Various clustering approaches based on distance and energy have been proposed, incorporating techniques such as flooding, fuzzy logic, and distributed methods for cluster head selection. These clustering algorithms, considering factors like distance, energy, sink node location, and node degree, aim to mitigate energy hole problem near the base station [22, 139–147].

In the context of 5G and beyond networks, researchers have incorporated ML algorithms, categorized as unsupervised, supervised, and reinforcement learning, for energy efficient and secure routing. Notably, these ML based algorithms are often compared with the conventional LEACH algorithm to assess performance. Swarm optimization [151], artificial neural networks [55, 152–154], self organizing neural network [155], fuzzy logic[156, 157], and differential evolution [108, 151] are among the ML based approaches explored for routing optimization,

overcoming redundancy, and addressing the energy hole problem. Researchers have showed the superior performance of these ML based algorithms compared to traditional clustering methods.

To enhance energy usage, energy efficient cluster head selection methods have been employed. However, as mentioned earlier, nodes closer to the base station tend to deplete their energy more rapidly, creating an undesirable energy hole. Researchers have considered parameters like distance, node degree, and energy for cluster head selection but have made weaker assumptions in their simulations, such as homogeneous node types and deployment in square fields [139–147]. Several other parameters, including the number of times a node becomes a cluster head, data transmission delay, load on a IoT device, imbalance in data communication, communication link, and SNR, may also influence cluster head selection but, to the best of authors knowledge, were not considered in the literature survey. Table 8 summarizes the parameters that may affect cluster head selection.

Tables 8 and 10 clearly show that parameters such as delay, load, CHC, imbalance in data communication, and SNR were not considered for the cluster head selection process. Typically, the selection of a cluster head within a cluster relied on three parameters (i.e. distance, node degree, and energy) or their variants in studies [139–147]. Table 9 provides insights into the simulation environment's characteristics, including node type, sink node location, and node deployment in the field. Moreover, table 10 briefly summarizes the research techniques, advantages, and limitations of these research works.

In resource constrained IoT environment, cluster based data forwarding approaches, utilizing clustering mechanisms like LEACH, facilitate data communication among cluster heads and base stations [146, 147]. The process becomes more complex with unequal cluster sizes, necessitating effective buffer management [141, 142]. Cluster heads store collected data in their buffers until transmitted to another cluster head, requiring knowledge of sleep and wake-up times [148, 149, 158]. Consequently, data is sent to the base station using multiple cluster heads, involving multi-hop communication due to the sensor's limited communication range [58, 73]. However, multi-hop communication introduces challenges such as identifying suitable active relay nodes, dealing with channel variability, addressing link disconnections, and managing low battery energy, all contributing to increased delay [58]. The frequency of use of closer cluster heads near the base station leads to rapid battery depletion, creating an energy hole problem. Numerous studies have focused on cluster head selection, aiming to maximize network lifetime and throughput.

As the IoT network experiences exponential growth in connected devices, short range communication technologies like Bluetooth, Wi-Fi, and radio frequency identification (i.e. RFID) are widely employed. The rise of 5G and beyond networks addresses challenges such as low data transmission rates, extensive device connectivity, high delay, low QoS, low throughput, and limited network capacity [66–73]. The research works highlighted the significance of 5G and beyond networks for applications like smart cities, smart health, and smart agriculture, characterized by substantial communication and computation requirements. Data offloading through D2D communication emerges as a solution to enhance energy efficiency, reduce link delays, widen coverage areas, offload data traffic, increase spectral efficiency, and boost data transmission rates. D2D communication facilitates direct device-to-device communication, eliminating the need for relay nodes or base stations, enhancing coverage, and relieving base stations by offloading data traffic [66–73].

ML techniques, when trained on extensive datasets, contribute to increasing the network's lifetime [36, 61, 64, 65]. ML models can predict prolonged network lifetime based on learned experiences, optimizing parameters such as data collection periodicity, D2D communication thresholds, and node degrees. Additionally, ML techniques applied to sensor collected data can identify correlations and aggregate correlated data before transmission, reducing communication,

Table 9 Summary of simulation parameters in energy efficient research works

S. No.	Reference No.	Simulation parameters		
		Node type	Node deployment in field	Sink node/ base station location
1.	[139]	Homogeneous	Square	Outside
2.	[140]	Homogeneous	Square	Outside
3.	[141]	Homogeneous	Square	Outside
4.	[142]	Homogeneous	Square	Outside
5.	[143]	Homogeneous	Square	Outside
6.	[144]	Homogeneous	Square	Outside
7.	[145]	Homogeneous	Square	Outside
8.	[146]	Homogeneous	Square	Inside
9.	[147]	Homogeneous	Square	Inside

Table 10 Summary of energy efficient research works [28]

S. No.	Reference No.	Technique	Advantage (+)	Limitation (-)
1.	[139]	Distance based clustering approach	Better than LEACH approach in energy consumption and network lifetime	· Distance, residual energy: ✓ · Node degree, delay, load, SNR: ×
2.	[140]	Distance based clustering approach	Better than study [139] in energy consumption	· Distance, residual energy: ✓ · Node degree, delay, load, SNR: ×
3.	[141]	Distance based clustering approach	Better than study [139] and LEACH in energy consumption	· Distance, residual energy: ✓ · Node degree, delay, load, SNR: ×
4.	[142]	Distance based clustering approach	Better than study [141] and LEACH in energy consumption	· CHC, base station location, load, delay, SNR: ×
5.	[143]	Distance based clustering approach	Outperforms study [139] in energy consumption and network lifetime	· Distance, base station location, residual energy: ✓ · Node degree, delay, load, SNR: ×
6.	[144]	Distance based clustering approach	Outperforms LEACH and work [141] in energy consumption and network lifetime	· CHC, base station location, load, delay: ×
7.	[145]	Distance based clustering approach	Better than studies [139, 140] and LEACH in energy consumption	· CHC, base station location, load, delay: ×
8.	[146]	Distance based clustering approach	Better than studies [139] and LEACH in energy consumption	· CHC, load, delay: ×
9.	[147]	Hierarchical clustering approach	Better than studies [141, 143] in energy consumption and network lifetime	· CHC, load, delay: ×

* Where ✓: Used for Cluster Head Selection, ×: Not Used for Cluster Head Selection

Table 11 Summary of Security Works

S. No.	Reference No.	IoT Domains					
		Smart grid	Smart home	Smart city	Smart healthcare	Smart parking	Smart agriculture
1.	[22]	×	×	✓	×	×	×
2.	[32]	✓	×	×	×	×	×
3.	[35]	✓	×	×	×	×	×
4.	[36]	×	×	×	×	×	✓
5.	[38]	×	×	×	✓	×	×
6.	[39]	×	×	×	✓	×	×
7.	[49]	×	×	×	✓	×	×
8.	[52]	×	×	×	✓	×	×
9.	[54]	✓	×	×	×	×	×
10.	[56]	✓	×	×	×	×	×
11.	[60]	×	×	✓	×	×	×
12.	[90]	×	×	✓	×	×	×
13.	[99]	×	×	✓	×	×	×
14.	[100]	✓	×	×	×	×	×
15.	[101]	×	✓	×	×	×	×
16.	[102]	×	✓	×	×	×	×
17.	[103]	×	✓	×	×	×	×
18.	[160]	×	✓	×	×	×	×

* Where ✓: Addressed, ×: Not Addressed

Table 12 Summary of privacy works

S. No.	Reference No.	IoT Domains					
		Smart grid	Smart home	Smart city	Smart healthcare	Smart parking	Smart agriculture
1.	[39]	×	×	×	✓	×	×
2.	[40]	×	✓	×	×	×	×
3.	[42]	✓	×	×	×	×	×
4.	[54]	×	×	✓	×	×	×
5.	[56]	✓	×	×	×	×	×
6.	[57]	✓	×	×	×	×	×
7.	[101]	×	✓	×	×	×	×
8.	[103]	×	✓	×	×	×	×

* Where ✓: Addressed, ×: Not Addressed

energy consumption, and improving performance. Despite the integration of D2D communication with IoT in 5G and beyond networks, challenges persist in resource allocation, interference management, security, mobility management, and mode selection. Effective solutions in these areas are crucial for maintaining direct connections, maximizing throughput, ensuring better QoS, managing interference, securing sensitive information, addressing mobility challenges, and optimizing resource utilization, especially in resource constrained IoT environments.

3.4 Security and privacy

Detecting potential attacks is a critical activity within a network, particularly in the context of an IoT network where the risk of unauthorized access to personal data presents a substantial threat to privacy [22, 30, 31]. Consequently, there is a growing emphasis on investigating privacy preserving mechanisms for IoT systems. In existing literature, researchers have introduced various techniques aimed at enhancing privacy [22, 39, 40, 42, 56, 57, 101, 103, 159] and providing adequate security [27, 36, 38, 39, 49, 52, 54, 56, 60, 81, 90, 99–101, 103, 160] in IoT communications. Notably, a majority

of these works concentrate on privacy concerns within applications such as smart grids and smart homes, while security considerations extend to applications in smart healthcare, smart cities, smart grids, and smart homes within the IoT environment. A detailed analysis in table 11 reveals that, out of 18 surveyed research works, only 1 addresses security concerns in smart agriculture, and none in smart parking. Similarly, table 12 highlights that, within the literature survey encompassing 8 research works, only 1 addresses privacy aspects in smart city, smart healthcare, and none in smart agriculture, smart parking.

The need of cost effective smart devices introduces security compromises, making hardware devices susceptible to various attacks, including side channel attacks and hardware trojans [31, 36]. Machine-to-machine communication emerges as a crucial element, facilitating the exchange of information among devices for collaborative operations [63, 71, 73]. Ensuring data privacy and confidentiality becomes imperative in this information sharing process, necessitating the implementation of cryptographic techniques to address security challenges [63]. The detection of attacks holds more importance in network security, particularly in the context of IoT networks where the potential leak of personal data poses a significant threat to privacy. To uphold data privacy, integrity, and secrecy during transmission, various cryptographic security techniques such as authentication, integrity, confidentiality, non-repudiation, and access control become essential. The implementation of such cryptographic security techniques on resource constrained devices, such as sensors, is a challenging task [41, 45]. Consequently, ensuring data privacy, integrity, and secrecy emerges as one of the most formidable tasks in the domain of smart IoT applications.

Privacy attacks typically focus on acquiring specific location and identity information of IoT devices, thereby compromising the system's privacy [43]. Identity privacy involves hiding the identities of message senders and receivers from third parties, including sender privacy, receiver privacy, and unlinkability between sender and receiver. Sensor privacy, equally crucial to sender and receiver privacy, prevents attackers from tracking sessions and executing attacks like sensor impersonation and sensor capture attacks. Attacks on location privacy, such as injecting false location information, may mislead autonomous systems like driverless tractors. In response, a three factor anonymous user authentication technique [161], employing the bio-hash function, ensures user anonymity and resilience against stolen mobile device attacks. Another framework [162] ensures non-repudiation, availability, authentication, and integrity through cross-domain resource access and integrity algorithms. Privacy preserving mechanisms, utilizing Elliptic Curve Cryptography [41] and ElGamal encryption [44], provide user and gateway anonymity. An additional technique [45] uses RSA and ElGamal cryptosystems to protect location and identity privacy, integrity, and message authenticity, despite incurring high communication costs and energy consumption. To address privacy concerns in edge enabled smart system, a privacy preserving data aggregation technique [46] combines signature mechanisms and Paillier homomorphic encryption for privacy preservation and integrity verification.

Detecting DoS attacks becomes essential task in resource constrained environments, as these attacks consume limited available resources such as memory, computing capabilities, and network capacity. A hybrid intrusion detection system (i.e. IDS) [163] classifies network traffic as attack or benign using decision trees and rule based principles. Another three layer IDS [164] employs supervised techniques to classify various cyber attacks, including replay attacks, DoS attacks, reconnaissance attacks, spoofing attacks, and person-in-the-middle attacks. An IDS presented in [165] detects active attacks and suspicious network activity, while an IDS [166] combines probability predictions from a tree of classifiers to identify cyber threats. Blockchain based solutions provide secure data processing and storage in fish farming [31], and an Ethereum blockchain security solution ensures traceability and trust in the agri-food supply chain [62]. A deep learning based IoT monitoring technique [167] utilizing disaggregation-aggregation architecture enhances security through audits and analytics. Operational threat and vulnerability evaluation approaches focusing on information assets provide a comprehensive perspective on security in smart agriculture [34]. In [168], symmetric cryptography and hash functions contribute to a secure user authenticated key management protocol, and in [169] distributed and clustered key management architecture assures secrecy through group based keys. Despite the promising prospects that new technologies bring to smart systems, they also introduce significant demands and challenges, particularly in terms of security and privacy. Table 13 and table 14 offer a summarized overview of privacy preserving solutions.

The privacy preserving works conducted in studies [41, 44–46] employ well known public cryptosystems like Elliptic Curve, RSA, and ElGamal. These cryptosystems, being computationally intensive, demand higher energy for their operations. Considering the resource constraints of smart devices and sensor nodes in smart system characterized by limited computational capabilities, there arises a necessity to employ lightweight cryptographic schemes to mitigate energy consumption. Surprisingly, to the best of authors knowledge, none of the research works in [41, 44–46] utilize lightweight cryptosystems. Resource constrained devices, such as smart cards, RFID tags, or sensors, may possess as little as $2KB$ and $1KB$ of Random Access Memory (i.e. RAM) and Electrically Erasable Programmable Read Only Memory (i.e.

Table 13 Summary of Security and Privacy Solutions

S. No.	Reference No.	Crypto-graphic Goal	Technique	Advantage (+)	Limitation (-)
1.	[41]	Privacy preserving	Elliptic curve cryptosystem utilized to provide user anonymity with untraceability, and gateway anonymity.	· Identity privacy with untraceability: ✓ · Gateway privacy: ✓ · Resistance against an attack on a loss mobile device: ✓ · Resistance against an attack on offline password guessing: ✓	· Location privacy: ×
2.	[43]	Privacy preserving	Proposed a dummy location privacy preserving mechanism. A dummy based approach creates a set of dummy locations for dummy users to hide real user's location	· Location privacy: ✓ · Security against inference attack: ✓ · Security against colluding attack: ✓	· Identity privacy: ×
3.	[44]	Privacy preserving	Auction based privacy preserving scheme is used to share the underutilized spectrum using Elgamal cryptosystem	· Identity privacy: ✓	· Location privacy: × · Spectrum heterogeneity: ×
4.	[45]	Privacy preserving	Modified Elgamal signature on elliptic curves is used to propose a secure and privacy preserving source anonymous message authentication scheme	· Location privacy: ✓ · Identity privacy: ✓ · Message authenticity and integrity: ✓ · Computation cost is low: ✓	· Commun-ication cost is very high · Energy consumption is more
5.	[46]	Privacy preserving	Paillier homomorphic encryption is used to propose a lightweight privacy preserving data aggregation scheme for edge computing enabled IoT system	· Identity privacy: ✓ · Integrity and unforgeability: ✓ · Authen-tication: ✓	· Location privacy: × · Security against collision attack: ×

* Where ✓: Provided, ×: Not Provided

Table 14 Summary of Offline/Online Design and Cryptosystem

S. No.	Reference No.	Cryptographic goal	Offline/ online design paradigm	Cryptosystem
1.	[41]	Privacy preserving	Does not use offline design paradigm	Uses Elliptic curve cryptosystem
2.	[44]	Privacy preserving	Does not use offline design paradigm	Uses Elgamal cryptosystem
3.	[45]	Privacy preserving	Uses offline and online design paradigm	Uses Elgamal cryptosystem
4.	[46]	Privacy preserving	Uses only online design paradigm	Uses Paillier homomorphic cryptosystem
5.	[43]	Privacy preserving	Uses only online design paradigm	-

EEPROM), respectively [43]. Performing cryptographic operations on such resource constrained devices with minimal energy consumption becomes crucial. Lightweight cryptography reduces the computational burden on devices and expands the applicability of conventional cryptography to resource constrained devices.

The adoption of an offline/online design paradigm proves advantageous in reducing computation costs while maintaining a low communication overhead [45]. In this paradigm, highly computational operations, such as those related to public key operations, can be performed during idle periods (i.e. offline mode) of a sensor node or smart device, while other operations can be executed when the device is engaged in data communication (i.e. online mode). In the reviewed literature on privacy preserving techniques [41, 43–46], all operations are mainly conducted in online mode, with the exception of [45], which intelligently integrates the offline/online design paradigm. However, despite successfully minimizing computation costs, the authors of [45] acknowledge a notable increase in communication costs, and it is essential to note that increase in communication costs correspond to higher energy consumption [27]. Table 15 illustrates the use of SDN, particularly in aspects of energy efficiency, security, privacy, scalability, interoperability, offloading, and heterogeneity.

4 Research gaps found in the literature survey

The authors discovered the following research gaps (i.e. RGs) in existing research works of literature survey. These RGs are studied in details in subsequent sections.

RG 1: Security and privacy consideration into frameworks and architectures
RG 2: Security and privacy in smart system
RG 3: Heterogeneity, Scalability and Interoperability
RG 4: Cloud and Edge Computing
RG 5: Lack of Appropriate Simulation Environment
RG 6: Lack of Parameters for Cluster Head Selection Method
RG 7: Energy Hole Problem
RG 8: Lightweight Cryptography
RG 9: Privacy Preserving
RG 10: Offline and Online Design Paradigm
RG 11: Imbalance Data Communication in Smart System
RG 12: Use of SDN, ML, Next Generation Wireless Network, Computer Vision, and D2D Communication

4.1 Security and privacy consideration into frameworks and architectures

Smart connected devices are the preferred option for attackers aiming to spread malware, viruses, and other security threats. Existing IoT security solutions have proven insufficient in securing against these evolving threats. Major players in the IoT industry are producing smart devices that, to gain a competitive edge in the open market, often lack adequate defenses against the latest security threats. Compounded by the fact that IoT devices typically operate with limited resources, traditional host based protection solutions like antivirus software, intrusion detection, and intrusion prevention systems face limitations. The emergence of advanced technologies introduce a novel networking paradigm designed to address the control, management, and security challenges inherent in conventional networking [101]. In response to the constraints imposed by resource limitations and evolving security threats in smart devices, there arises a need for

Table 15 Summary of Use of SDN in energy efficiency, privacy, security, offloading, scalability, heterogeneity, imbalance load

S. No.	Research area	Addressed or not	Why do we want to consider
1.	Energy Consumption [22, 27, 29, 33]	Yes but SDN is not used	There is a scope to propose an incremental solution for finding energy efficient paths in IoT networks considering device failures utilizing SDN
2.	Load Imbalance in Data Communication [22]	Not Addressed	There is a scope to take this load imbalance factor into account and design a mechanism/algorithm utilizing the principles of SDN
3.	Offloading [22, 36, 58, 106]	Yes but SDN is not used	There is a scope to explore the feasibility of using data plane programmable switches for data offloading and quick response times in data processing utilizing SDN
4.	Privacy [39, 40, 42] and Security [27, 36, 38, 49, 54, 60, 81, 90, 101]	Yes but in limited domains and SDN is not used	There is a scope to work on designing a solution for privacy and security in an unexplored domain/application utilizing the principles of SDN
5.	Scalability [27], and Heterogeneity [27, 33]	Yes but in limited extent and SDN is not used	There is a scope to utilize the principles of SDN and find a scalable solution to handle large numbers of IoT devices and IoT traffic

an architecture that can provide security leveraging lightweight cryptographic parameters. The authors also identify the absence of a standard framework and architecture for smart IoT systems, emphasizing the need for considerations related to security, privacy, and energy optimization. The inadequacy of most presented frameworks and architectures in accounting for energy efficiency, security, and privacy issues is evident in table 6 and table 7. Consequently, there is a gap in the consideration of security, energy management, and privacy aspects within the frameworks and architectures of smart systems. This highlights the opportunity to develop a comprehensive and generic framework or architecture that explicitly incorporates security, energy management, and privacy considerations, leveraging several advanced technologies as discussed in the section 4.12.

4.2 Security and privacy in smart system

The primary objective of a smart system is to significantly enhance the QoS for its citizens and maximize the utilization of available assets and resources sustainably. Data acquisition is essential to facilitate real time and intelligent decision making for various activities. Companies are eager to develop products to capture the growing domestic IoT market, yet security features are often overlooked, resulting in a sudden increase of vulnerable IoT devices. One of the significant challenges in realizing the smart system concept lies in the secure and efficient distribution and management of the exponentially increasing volume of data. Detecting attacks is a essential activity in any network, and it becomes even more crucial in an IoT network due to the substantial risk of personal data leakage leading to privacy violations. Existing literature has proposed various techniques for privacy [22, 39, 40, 42, 56, 57, 101, 103] and security [27, 36, 38, 39, 49, 52, 54, 56, 60, 81, 90, 99–101, 103, 160] in IoT communications, with a predominant focus on smart grids and smart healthcare applications. Table 11 reveals that researchers have addressed security concerns in smart city, smart grid, smart home, and smart healthcare domains to the required extent. However, security considerations in other domains, such as smart agriculture and smart parking, have been neglected. Similarly, table 12 indicates that privacy concerns in the IoT domain have been adequately addressed in smart grid and smart home applications, and to a basic extent in smart city and smart health. However, domains like smart agriculture and smart parking have been overlooked in terms of privacy. Therefore, there is an evident opportunity to develop a solution that considers security and privacy in unexplored domains or applications, such as smart agriculture, leveraging advanced technologies as discussed in the section 4.12.

4.3 Heterogeneity, scalability and interoperability

In pursuit of optimal battery life, researchers have employed methodologies such as cluster based data transmission [36] and sleep-wake techniques [65]. However, these approaches exhibit shortcomings in terms of interoperability [63, 149], lack of diversity [63], and high energy consumption rates [63]. Furthermore, these techniques often overlook the heterogeneous nature of the IoT environment [63, 64]. A detailed literature survey, as depicted in table 6 and table 7, highlights a critical gap in the analysis of heterogeneity and scalability/interoperability issues in IoT based systems, particularly concerning the diversity of devices supported by the network. Consequently, there exists an opportunity to leverage advanced technologies and devise a scalable solution capable of effectively managing a substantial number of IoT devices and handling the associated IoT traffic.

4.4 Cloud and edge computing

The cloud serves as an exemplary platform for analytical processes, with IoT device data routed to the cloud for decision making and historical analysis. Among the basic operations such as data gathering, collection, and processing, the latter is executed by processing units/servers to derive decisions and conduct analyses. Timely processing of data is crucial for accurate decision making and observations. Physical sensors in the environment detect data based on their attached sources and transmit these values to the cloud. To quick data processing, researchers have used the combination of edge computing and cloud computing [31, 36, 62, 147]. However, it is noteworthy that data processing in the cloud is associated with huge energy consumption, attributed to escalating transmission costs and latency. Additionally, significant portions of IoT device energy are consumed in activities such as data collisions, re-transmission, sensing, transmitting, and receiving [63]. Consequently, there exists an opportunity to investigate data analysis at the edge or within fog computing frameworks, leveraging advanced technologies to optimize energy usage and reduce latency.

4.5 Lack of appropriate simulation environment

In the literature survey, as mentioned in table 9 and table 10, research works [22, 139–147] on energy efficiency mainly incorporated a homogeneous node type within their simulation models. Furthermore, these research works exclusively deployed nodes in square fields during their simulation processes. Notably, the literature lacks instances where non-homogeneous node types and non-square deployment fields were employed in these simulations. Additionally, as presented in table 9 and table 10, the evaluation of sink node locations in the works [139–146] on energy efficiency indicated that the sink node was consistently positioned outside the fields. Only two research works [22, 147] considered the placement of sink nodes within the simulation environment. Consequently, there exists an opportunity to explore simulations involving non-homogeneous node types and non-square deployment fields, as well as to investigate the implications of sink node locations both inside and outside the fields, leveraging advanced technologies for comprehensive analysis.

4.6 Lack of parameters for cluster head selection method

In the literature survey, as mentioned in table 8 and table 10, research works on energy efficiency [22, 139–147] have uniformly relied upon the selection of cluster heads based on several parameters such as distance, residual energy, and node degree. Significantly, the current state of research, to the best of authors knowledge, reveals an absence of works employing parameters beyond these three or their variants for the purpose of cluster head selection within a cluster. This gap in the existing works suggests an exploration of diverse parameters, including but not limited to load, CHC, delay, SNR, either individually or in a combination, could be employed to design an intelligent and energy efficient mechanism within smart IoT systems by leveraging advanced technologies.

4.7 Energy hole problem

Based on an extensive review of the literature [66–73], it is found out that multi-hop communication is essential for transmitting data to the base station, primarily due to the limited communication range of sensors. However, the utilization of multi-hop communication introduces a list of drawbacks, including a lack of suitable active relay nodes, channel variability, link disconnection, and low battery energy, all of which collectively contribute to a delay in transmitting data from sensor nodes to the base station. Furthermore, the frequency with which cluster heads nearer to the base station are used surpasses that of their more distant counterparts, thereby accelerating the rate of battery depletion for the former, thereby leading an energy hole problem. The authors observed that within the context of the smart IoT environment, there exists a practice wherein, to save energy consumption, sensors occasionally avoid using direct transmission to processing units or servers. Instead, they relay data to intermediary IoT devices, which subsequently undertake the transmission to processing units. Regrettably, the issue of intermediary forwarding devices failing due to battery drainage remains unaddressed in extant literature focused on computing energy efficient paths [36]. Consequently, an unexplored area for research, justifying the development of an incremental algorithm to find out the energy efficient paths within IoT networks. Importantly, this algorithm should account for potential failures of intermediary devices, thereby necessitating the incorporation of advanced technologies to strengthen the robustness of the proposed algorithm.

4.8 Lightweight cryptography

In the literature survey, as described in table 13 and table 14, the research studies on privacy preserving [41, 44–46] use public cryptosystems such as RSA and Elgamal. However, these public cryptosystems are computationally heavy, therefore they require more energy to perform their operations. To the best of authors knowledge, none of these research works [41, 44–46] use lightweight cryptosystems. Hence, there is a scope to work on designing the lightweight cryptosystems for providing security and privacy in smart IoT networks utilizing advanced technologies.

4.9 Privacy preserving

From the literature review, as presented in table 13, to the best of authors knowledge, none of the research works on privacy preserving [41, 43–46], except [45], provide both the identity and location privacy. Only one research study [45] provides both identity and location privacy. However, in this study [45], the energy consumption is more

since communication cost is huge. Thus, there is no research work which can provide both identity and location privacy while maintaining a low energy consumption. Therefore, there is a scope to work on designing and developing an intelligent mechanism for enabling both identity and location privacy preservation in smart IoT systems by leveraging the advanced technologies.

4.10 Offline and online design paradigm

It is inferred by the literature study, as mentioned in table 14, to the best of authors knowledge, none of the research works on privacy preserving [41, 43–46], except [45], use the offline/online design paradigm. However, the study [45] used the offline/online design paradigm but the communication cost was very high while the authors were able to maintain a low computation cost. When communication costs are very high, energy consumption will be more [27]. Hence, there is a scope to use offline/online design paradigm in the smart IoT system for designing and developing a privacy preserving mechanism to reduce the energy consumption.

4.11 Imbalance data communication in smart system

An imbalance communication may impact an energy/power constraint environment like an IoT network [22]. The imbalance data communication occurs in IoT because some sensors are used for inter-cluster communication while others used for intra-cluster communication that leads to an unwanted energy hole problem [66–73]. It is observed in the literature survey that the issue of imbalance data communications leads to the energy hole problem which ultimately makes the network unstable. Hence, there is a scope to take this load imbalance factor into account and design a mechanism utilizing the principles of advanced technologies that will balance out the load on the IoT devices in terms of communication.

4.12 Use of SDN, ML, next generation wireless network, computer vision, and D2D communication

There is a scope to process or analyze the collected data by using the ML techniques before sending this collected data to the base station [36, 61, 63–65]. During such processing, the ML techniques can find some correlations between collected data and can make an aggregated form of the correlated data before sending it to the base station. Thus, by doing so the communications can be reduced which reduces energy consumption and improves performance. From the works [36, 61, 63–65], the authors found that there is a scope to use ML techniques to assist in increasing the network's lifetime. These techniques may predict extended periods of network lifetime based on their learned experience such as periodicity of data collection, threshold value for D2D communication, and node degree etc. It is also inferred by the literature studies such as [66–73] that there is a scope to use next generation wireless networks such as 5G and beyond to address several issues such as low data transmission rate, massive device connectivity, high delay, low QoS, low throughput, and low network capacity etc. Hence, integration of the D2D communication with IoT through next generation networks may improve energy efficiency, provide wide coverage area, and offload data traffic. Also, there is a scope to explore the feasibility of programmable switches for data offloading and quick response times in data processing utilizing SDN. The advanced technologies such as fog computing, cloud computing, big data, 5G and beyond, D2D communications, SDN, NFV, AI, computer vision, and ML can all be integrated into IoT to extend its functionality.

5 Conclusion and future scope

This present research work explored various critical factors and issues including QoS, energy efficiency, security and privacy, resource management, energy consumption, heterogeneity, scalability, and interoperability within resource constrained smart IoT systems such as smart health, smart grid, smart city, smart parking, smart agriculture, and smart home etc. A substantially detailed review of the existing research works in each of these domains has been conducted, highlighting relevant issues such as energy challenges, security concerns, privacy concerns, and heterogeneity related complexities.

The current study presents several key findings that are summarized as follows:

- A lack of a standardized frameworks and architecture for smart IoT systems has been identified, in spite of the existence of multiple frameworks and architectures, which, unfortunately, often overlook security and privacy considerations.
- Security issues are addressed across various domains, but not consistently, and this inconsistency also applies to privacy. Consequently, there is a clear opportunity to develop solutions that consider security and privacy in areas that have not yet been fully explored.
- A significant gap exists in the analysis of heterogeneity, scalability, and interoperability issues in IoT based systems, particularly regarding the variety of devices supported by the network. This presents an opportunity to develop a scalable solution that can effectively manage a large number of IoT devices and handle the associated traffic.
- Data processing in the cloud involves substantial energy consumption, largely due to increasing transmission costs and latency. Additionally, IoT devices consume a significant amount of energy. This creates an opportunity to explore data analysis within computing frameworks to optimize energy usage and reduce latency.
- Research works on energy efficiency consistently focuses on selecting cluster heads based on distance, residual energy, and node degree. This gap indicates the potential to develop an energy efficient mechanism in smart IoT systems by considering a broader range of parameters, such as load, CHC, delay, and SNR, either individually or in combination.
- Research studies on privacy preservation typically utilize public cryptosystems like RSA and Elgamal. However, these cryptosystems are computationally intensive and require significant energy to operate. Consequently, there is a need to develop lightweight cryptosystems to provide security and privacy in smart IoT networks.
- There is also a potential to apply the offline/online design paradigm in smart IoT systems to develop privacy preserving mechanisms that reduce energy consumption.
- The present study also recognizes the potential impact of advanced technologies like SDN, ML, 5G, D2D communication, big data, cloud computing, computer vision, and edge computing in enhancing the capabilities of the smart systems.

Future research should focus on developing an intelligent, energy efficient, privacy preserving, and secure data transmission mechanism tailored for D2D communication in smart IoT systems operating within the coverage of 5G and beyond networks. Such a mechanism should dynamically adapt to network conditions, optimize energy consumption, and ensure both security and privacy while facilitating seamless communication between IoT devices. Additionally, there is a need to design a lightweight, intelligent privacy preserving mechanism that can effectively address the challenges of resource constrained smart IoT environments. This mechanism should minimize computational overhead while maintaining robust security and privacy protections, making it suitable for IoT applications with limited processing power and energy resources. Furthermore, future studies should focus on developing an energy efficient, secure, and privacy preserving framework that is adaptable to the diverse requirements of various smart IoT systems. Since different smart applications have unique constraints and priorities, this framework should be flexible enough to balance energy efficiency, security, and privacy based on the specific needs of each system. By addressing these challenges, future research can contribute to the advancement of secure and efficient data communication in next-generation IoT networks.

Acknowledgements The authors are thankful to the anonymous reviewers and editor for their invaluable feedback.

Author contributions The conception and design of the study were primarily carried out by Shreeram Hudda, who also took the lead in drafting the initial version of the manuscript. K. Haribabu provided guidance on the research methodology, supervised the technical aspects of the work, refined the manuscript, and contributed to the interpretation of results. The final draft of the manuscript was reviewed, critically revised, and approved by all authors, ensuring their collective agreement and contribution to the work presented.

Funding Open access funding provided by Birla Institute of Technology and Science. The authors are thankful to Birla Institute of Technology & Science - Pilani (BITS - Pilani) for funding this work.

Data availability No datasets are generated or analysed during the current study.

Declarations

Ethics approval and consent to participate Not applicable

Consent for Publication Not applicable

Competing Interests The authors have no conflicts of interest to declare that are relevant to the content of this article.

References

1. Wang Q, Balasingham I. Wireless sensor networks-an introduction. Wireless Sensor Netw Appl Centric Design. 2010;10:1–14.
2. Dargie W, Poellabauer C. Fundamentals of Wireless Sensor Networks: Theory and Practice. John Wiley & Sons; 2010.
3. Sohraby K, Minoli D, Znati T. Wireless Sensor Networks: Technology, Protocols, and Applications. John wiley & sons; 2007.
4. Fischione C. An introduction to wireless sensor networks. Royal Institute of technology. Draft, version 1 2014.
5. Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, p. 10. IEEE Comput. Soc, 2000. https://doi.org/10.1109/hicss.2000.926982 .
6. Misra S, Mukherjee A, Roy A. Introduction IoT. Cambridge University Press; 2021.
7. Lea P. Internet of Things for Architects: Architecting IoT Solutions by Implementing Sensors, Communication Infrastructure Edge Computing: Analytics, and Security. Birmingham: Packt Publishing Ltd; 2018.
8. Khanna A, Kaur S. Internet of things (iot), applications and challenges: a comprehensive review. Wireless Personal Commun. 2020;114:1687–762. https://doi.org/10.1007/s11277-020-07446-4.
9. Lakhwani K, Gianey HK, Wireko JK, Hiran KK. Internet of Things (IoT): Principles. Paradigms and Applications of IoT: Bpb Publications, 2020.
10. Hanes D, Salgueiro G, Grossetete P, Barton R, Henry J. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. Indianapolis: Cisco Press; 2017.
11. Sindhwani N, Anand R, Niranjanamurthy M, Verma DC, Valentina EB. IoT Based Smart Applications. Boca Raton: Springer; 2023.
12. Tripathy B, Anuradha J. Internet of Things (IoT): Technologies, Applications, Challenges and Solutions. Boca Raton: CRC Press; 2017.
13. Khan JY, Yuce MR. Internet of Things (IoT): Systems and Applications. Boca Raton: CRC Press; 2019.
14. Khang A, Abdullayev V, Hahanov V, Shah V. Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy. Boca Raton: CRC Press; 2024.
15. Hassan QF. Internet of Things A to Z: Technologies and Applications. Hoboken: John Wiley & Sons; 2018.
16. Yang K. Wireless Sensor Networks. Berlin: Springer; 2014.
17. Nagaraj A. Introduction to Sensors in IoT and Cloud Computing Applications. Sharjah: Bentham Science Publishers; 2021.
18. Rani S, Maheswar R, Kanagachidambaresan G, Jayarajan P. Integration of WSN and IoT for smart cities. Berlin: Springer; 2020.
19. Mukherjee P, Pattnaik PK, Panda SN. Iot and wsn applications for modern agricultural advancements: emerging research and opportunities: Emerging research and opportunities 2019.
20. Wu F, Rüdiger C, Yuce MR. Real-time performance of a self-powered environmental iot sensor network system. Sensors. 2017;17(2):282.
21. Hudda S, Haribabu K, Barnwal R, Khurana A. A wsn and vision based energy efficient and smart surveillance system using computer vision and ai at edge. In: 2024 International Conference on Advanced Information Networking and Applications (AINA), pp. 24–36 2024. https://doi.org/10.1007/978-3-031-57870-0_3 . Springer.
22. Islam MJ, Rahman A, Kabir S, Karim MR, Acharjee UK, Nasir MK, Band SS, Sookhak M, Wu S. Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities. IEEE Int Things J. 2022;9(5):3850–64. https://doi.org/10.1109/jiot.2021.3100797.
23. Meenakshi N, Ahmad S, Prabu A, Rao JN, Othman NA, Abdeljaber HA, Sekar R, Nazeer J. Efficient communication in wireless sensor networks using optimized energy efficient engroove leach clustering protocol. Tsinghua Sci Technol. 2024;29(4):985–1001. https://doi.org/10.26599/TST.2023.9010056.
24. Gururaj H, Natarajan R, Almujally NA, Flammini F, Krishna S, Gupta SK. Collaborative energy-efficient routing protocol for sustainable communication in 5g/6g wireless sensor networks. IEEE Open J Commun Soc. 2023. https://doi.org/10.1109/OJCOMS.2023.3312155.
25. Saleem K, Wang L, Bharany S, Ouahada K, Rehman AU, Hamam H. Intelligent multi-agent model for energy-efficient communication in wireless sensor networks. EURASIP J Inform Security. 2024;2024(1):9. https://doi.org/10.1186/s13635-024-00155-6.
26. Nieto RM, García-Martin Á, Hauptmann AG, Martínez JM. Automatic vacant parking places management system using multicamera vehicle detection. IEEE Trans Intell Transport Syst. 2019;20(3):1069–80. https://doi.org/10.1109/TITS.2018.2838128. (**IEEE**).
27. Rana B, Singh Y, Singh PK. A systematic survey on internet of things: energy efficiency and interoperability perspective. Trans Emerg Telecommun Technol. 2020. https://doi.org/10.1002/ett.4166.
28. Hudda S, Haribabu K, Barnwal R. Energy efficient data communication for wsn based resource constrained iot devices. Int Things. 2024;27:101329. https://doi.org/10.1016/j.iot.2024.101329.
29. Haimour J, Abu-Sharkh O. Energy efficient sleep/wake-up techniques for iot: A survey. In: 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 478–484. IEEE, 2019. https://doi.org/10.1109/jeeit.2019.8717372 .
30. Hurrah NN, Parah SA, Sheikh JA, Al-Turjman F, Muhammad K. Secure data transmission framework for confidentiality in iots. Ad Hoc Networks. 2019;95: 101989. https://doi.org/10.1016/j.adhoc.2019.101989.

31. Hang L, Ullah I, Kim D-H. A secure fish farm platform based on blockchain for agriculture data integrity. Computers Electron Agric. 2020;170: 105251. https://doi.org/10.1016/j.compag.2020.105251.
32. Zhuang P, Liang H. False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks. IEEE Trans Smart Grid. 2020;12(3):2566–77. https://doi.org/10.1109/TSG.2020.3042926.
33. Jiang C, Fan T, Gao H, Shi W, Liu L, Cérin C, Wan J. Energy aware edge computing: a survey. Computer Communications. 2020;151:556–80. https://doi.org/10.1016/j.comcom.2020.01.004.
34. Ali B, Awad A. Cyber and physical security vulnerability assessment for iot-based smart homes. Sensors. 2018;18(3):817. https://doi.org/10.3390/s18030817.
35. Chaudhary R, Aujla GS, Garg S, Kumar N, Rodrigues JJ. Sdn-enabled multi-attribute-based secure communication for smart grid in iot environment. IEEE Trans Industrial Informatics. 2018;14(6):2629–40. https://doi.org/10.1109/TII.2018.2789442.
36. Friha O, Ferrag MA, Shu L, Nafa M. A robust security framework based on blockchain and sdn for fog computing enabled agricultural internet of things. In: 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), pp. 1–5 2020. https://doi.org/10.1109/ITIA50152.2020.9312286 . IEEE.
37. Kim Y, Nam J, Park T, Scott-Hayward S, Shin S. Soda: A software-defined security framework for iot environments. Computer Netw. 2019;163: 106889. https://doi.org/10.1016/j.comnet.2019.106889.
38. Li J, Cai J, Khan F, Rehman AU, Balasubramaniam V, Sun J, Venu P. A secured framework for sdn-based edge computing in iot-enabled healthcare system. IEEE Access. 2020;8:135479–90. https://doi.org/10.1109/ACCESS.2020.3011503.
39. Jiang S, Duan M, Wang L. Toward privacy-preserving symptoms matching in sdn-based mobile healthcare social networks. IEEE Int Things J. 2018;5(3):1379–88. https://doi.org/10.1109/JIOT.2018.2799209.
40. Pinheiro AJ, Araujo-Filho PF, Bezerra JDM, Campelo DR. Adaptive packet padding approach for smart home networks: a tradeoff between privacy and performance. IEEE Int Things J. 2020;8(5):3930–8. https://doi.org/10.1109/JIOT.2020.3025988.
41. Shin S, Kwon T. A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5g-integrated internet of things. IEEE Access. 2020;8:67555–71. https://doi.org/10.1109/access.2020.2985719.
42. Sivaraman V, Sikdar B. A game-theoretic approach for enhancing data privacy in sdn-based smart grids. IEEE Int Things J. 2020;8(13):10583–95. https://doi.org/10.1109/JIOT.2020.3048357.
43. Sun G, Chang V, Ramachandran M, Sun Z, Li G, Yu H, Liao D. Efficient location privacy algorithm for internet of things (iot) services and applications. J Netw Computer Appl. 2017;89:3–13. https://doi.org/10.1016/j.jnca.2016.10.011.
44. Wang X, Umehira M, Han B, Zhou H, Li P, Wu C. An efficient privacy preserving spectrum sharing framework for internet of things. IEEE Access. 2020;8:34675–85. https://doi.org/10.1109/access.2020.2974227.
45. Wei J, Phuong TVX, Yang G. An efficient privacy preserving message authentication scheme for internet-of-things. IEEE Trans Indust Inform. 2021;17(1):617–26. https://doi.org/10.1109/tii.2020.2972623.
46. Zhang J, Zhao Y, Wu J, Chen B. Lvpda: a lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled iot. IEEE Int Things J. 2020;7(5):4016–27. https://doi.org/10.1109/jiot.2020.2978286.
47. Baktir AC, Tunca C, Ozgovde A, Salur G, Ersoy C. Sdn-based multi-tier computing and communication architecture for pervasive healthcare. IEEE Access. 2018;6:56765–81. https://doi.org/10.1109/ACCESS.2018.2873907.
48. Gia TN, Rahmani A-M, Westerlund T, Liljeberg P, Tenhunen H. Fault tolerant and scalable iot-based architecture for health monitoring. In: 2015 IEEE Sensors Applications Symposium (SAS). IEEE, 2015. https://doi.org/10.1109/sas.2015.7133626 .
49. Meng Y, Huang Z, Shen G, Ke C. Sdn-based security enforcement framework for data sharing systems of smart healthcare. IEEE Trans Netw Service Manage. 2019;17(1):308–18. https://doi.org/10.1109/TNSM.2019.2941214.
50. Misra S, Saha R, Ahmed N. Health-flow: Criticality-aware flow control for sdn-based healthcare iot. In: GLOBECOM 2020-2020 IEEE Global Communications Conference, pp. 1–6 2020. https://doi.org/10.1109/GLOBECOM42002.2020.9348058 . IEEE.
51. Sallabi F, Naeem F, Awad M, Shuaib K. Managing iot-based smart healthcare systems traffic with software defined networks. In: 2018 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6 2018. https://doi.org/10.1109/ISNCC.2018.8530920 . IEEE.
52. Srilakshmi A, Mohanapriya P, Harini D, Geetha K. Iot based smart health care system to prevent security attacks in sdn. In: 2019 Fifth International Conference on Electrical Energy Systems (ICEES), pp. 1–7 2019. https://doi.org/10.1109/ICEES.2019.8719236 . IEEE.
53. Verma P, Sood SK. Cloud-centric iot based disease diagnosis healthcare framework. J Parallel Distributed Comput. 2018;116:27–38. https://doi.org/10.1016/j.jpdc.2017.11.018.
54. Soares AA, Lopes Y, Passos D, Fernandes NC, Muchaluat-Saade DC. 3as: authentication, authorization, and accountability for sdn-based smart grids. IEEE Access. 2021;9:88621–40. https://doi.org/10.1109/ACCESS.2021.3090346.
55. Sharma VK, Shukla SSP, Singh V. A tailored q- learning for routing in wireless sensor networks. In: 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing. IEEE, 2012. https://doi.org/10.1109/pdgc.2012.6449899 .
56. Rehmani MH, Davy A, Jennings B, Assi C. Software defined networks-based smart grid communication: a comprehensive survey. IEEE Commun Surv & Tutorials. 2019;21(3):2637–70. https://doi.org/10.1109/COMST.2019.2908266.
57. Lv Z, Wang L, Guan Z, Wu J, Du X, Zhao H, Guizani M. An optimizing and differentially private clustering algorithm for mixed data in sdn-based smart grid. IEEE access. 2019;7:45773–82. https://doi.org/10.1109/ACCESS.2019.2909048.
58. Lalle Y, Fourati M, Fourati LC, Barraca JP. Routing strategies for lorawan multi-hop networks: a survey and an sdn-based solution for smart water grid. IEEE Access. 2021;9:168624–47. https://doi.org/10.1109/ACCESS.2021.3135080.
59. Jakaria A, Rahman MA, Gokhale A. Resiliency-aware deployment of sdn in smart grid scada: a formal synthesis model. IEEE Trans Net Service Management. 2021;18(2):1430–44. https://doi.org/10.1109/TNSM.2021.3050148.
60. Aujla GS, Singh M, Bose A, Kumar N, Han G, Buyya R. Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications. IEEE Netw. 2020;34(2):83–91. https://doi.org/10.1109/MNET.001.1900151.
61. Friha O, Ferrag MA, Shu L, Maglaras L, Wang X. Internet of things for the future of smart agriculture: a comprehensive survey of emerging technologies. IEEE/CAA Journal of Automatica Sinica. 2021;8(4):718–52. https://doi.org/10.1109/JAS.2021.1003925.
62. Shahid A, Almogren A, Javaid N, Al-Zahrani FA, Zuair M, Alam M. Blockchain-based agri-food supply chain: a complete solution. IEEE Access. 2020;8:69230–43. https://doi.org/10.1109/access.2020.2986257.

63. Singh RK, Berkvens R, Weyn M. Agrifusion: an architecture for iot and emerging technologies based on a precision agriculture survey. IEEE Access. 2021;9:136253–83. https://doi.org/10.1109/ACCESS.2021.3116814.
64. Verdouw C, Sundmaeker H, Tekinerdogan B, Conzon D, Montanaro T. Architecture framework of iot-based food and farm systems: a multiple case study. Computer Electron Agric. 2019;165: 104939. https://doi.org/10.1016/j.compag.2019.104939.
65. Alonso RS, Sittón-Candanedo I, Casado-Vara R, Prieto J, Corchado JM. Deep reinforcement learning for the management of software-defined networks in smart farming. In: 2020 International Conference on Omni-layer Intelligent Systems (COINS), pp. 1–6 2020. https://doi.org/10.1109/COINS49042.2020.9191634 . IEEE.
66. Zhang Y, Wu G, Deng L, Fu J. Arrival rate-based average energy-efficient resource allocation for 5g heterogeneous cloud ran. IEEE Access. 2019;7:136332–42. https://doi.org/10.1109/ACCESS.2019.2939348.
67. Shi J, Yu W, Ni Q, Liang W, Li Z, Xiao P. Energy efficient resource allocation in hybrid non-orthogonal multiple access systems. IEEE Trans Commun. 2019;67(5):3496–511. https://doi.org/10.1109/TCOMM.2019.2893304.
68. Kuang Z, Liu G, Li G, Deng X. Energy efficient resource allocation algorithm in energy harvesting-based d2d heterogeneous networks. IEEE Int Things J. 2018;6(1):557–67. https://doi.org/10.1109/JIOT.2018.2842738.
69. Zhang H, Fang F, Cheng J, Long K, Wang W, Leung VC. Energy-efficient resource allocation in noma heterogeneous networks. IEEE Wireless Commun. 2018;25(2):48–53. https://doi.org/10.1109/MWC.2018.1700074.
70. Amani N, Pedram H, Taheri H, Parsaeefard S. Energy-efficient resource allocation in heterogeneous cloud radio access networks via bbu offloading. IEEE Trans Vehic Technol. 2018;68(2):1365–77. https://doi.org/10.1109/TVT.2018.2882466.
71. Guo S, Zhou X, Xiao S, Sun M. Fairness-aware energy-efficient resource allocation in d2d communication networks. IEEE Syst J. 2018;13(2):1273–84. https://doi.org/10.1109/JSYST.2018.2838539.
72. Abbas F, Fan P, Khan Z. A novel low-latency v2v resource allocation scheme based on cellular v2x communications. IEEE Trans Intell Transport Syst. 2018;20(6):2185–97. https://doi.org/10.1109/TITS.2018.2865173.
73. Alwan S, Fajjari I, Aitsaadi N. D2d multihop energy-efficient routing and ofdma resource allocation in 5g networks. In: 2018 IFIP Networking Conference (IFIP Networking) and Workshops, pp. 1–9. IEEE, 2018. https://doi.org/10.23919/IFIPNetworking.2018.8696917 .
74. Hudda S, Barnwal R, Khurana A, Haribabu K. A wsn and vision based smart, energy efficient, scalable, and reliable parking surveillance system with optical verification at edge for resource constrained iot devices. Int Things. 2024;28: 101346. https://doi.org/10.1016/j.iot.2024.101346.
75. Kurose J, Ross K. Computer Networking: A Top-down Approach. Pearson, 2021. [Online]: https://gaia.cs.umass.edu/kurose_ross/online_lectures.htm, Last Accessed 20-09-2024
76. McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Shenker S, Turner J. Openflow: enabling innovation in campus networks. ACM SIGCOMM Computer Commun Rev. 2008;38(2):69–74. https://doi.org/10.1145/1355734.1355746.
77. Li W, Meng W, Kwok LF. A survey on openflow-based software defined networks: security challenges and countermeasures. J Netw Computer Appl. 2016;68:126–39. https://doi.org/10.1016/j.jnca.2016.04.011.
78. Bosshart P, Daly D, Gibb G, Izzard M, McKeown N, Rexford J, Schlesinger C, Talayco D, Vahdat A, Varghese G, Walker D. P4: programming protocol-independent packet processors. ACM SIGCOMM Computer Commun Rev. 2014;44(3):87–95. https://doi.org/10.1145/2656877.2656890.
79. Chen N, Wang M, Zhang N, Shen XS, Zhao D. Sdn-based framework for the pev integrated smart grid. Ieee Netw. 2017;31(2):14–21. https://doi.org/10.1109/MNET.2017.1600212NM.
80. Chekired DA, Khoukhi L, Mouftah HT. Decentralized cloud-sdn architecture in smart grid: a dynamic pricing model. IEEE Trans Indust Inform. 2017;14(3):1220–31. https://doi.org/10.1109/TII.2017.2742147.
81. Al-Rubaye S, Kadhum E, Ni Q, Anpalagan A. Industrial internet of things driven by sdn platform for smart grid resiliency. IEEE Int Things J. 2017;6(1):267–77. https://doi.org/10.1109/JIOT.2017.2734903.
82. Lopes Y, Fernandes NC, Muchaluat-Saade DC, Obraczka K. Ares: An autonomic and resilient framework for smart grids. In: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 222–229 2017. https://doi.org/10.23919/INM.2017.7987283 . IEEE.
83. Overview of Smart Grid Technology And Its Operation and Application (For Existing Power System). ElProCus Technologies Pvt Ltd. [Online]: https://www.elprocus.com/overview-smart-grid-technology-operation-application-existing-power-system/, Last Accessed 20-09-2024
84. Azlin AAN, Mansor H, Hashim AZ, Gunawan TS. Development of modular smart farm system. In: 2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA), pp. 1–6 2017. https://doi.org/10.1109/ICSIMA.2017.8312019 . IEEE.
85. Ordoñez-García A, Siller M, Begovich O. Iot architecture for urban agronomy and precision applications. In: 2017 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), pp. 1–4 2017. https://doi.org/10.1109/ROPEC.2017.8261582 . IEEE.
86. Rehman A, Saba T, Kashif M, Fati SM, Bahaj SA, Chaudhry H. A revisit of internet of things technologies for monitoring and control strategies in smart agriculture. Agronomy. 2022;12(1):127. https://doi.org/10.3390/agronomy12010127.
87. Xu K, Wang X, Wei W, Song H, Mao B. Toward software defined smart home. IEEE Commun Magazine. 2016;54(5):116–22. https://doi.org/10.1109/MCOM.2016.7470945.
88. Kadir K, Yusof ZM, Rasin MZM, Billah MM, Salikin Q. Wireless imu: a wearable smart sensor for disability rehabilitation training. In: 2018 2nd International Conference on Smart Sensors and Application (ICSSA), pp. 53–57 2018. https://doi.org/10.1109/ICSSA.2018.8535952 . IEEE.
89. Jawad N, Salih M, Ali K, Meunier B, Zhang Y, Zhang X, Zetik R, Zarakovitis C, Koumaras H, Kourtis M-A, et al. Smart television services using nfv/sdn network management. IEEE Trans Broadcast. 2019;65(2):404–13. https://doi.org/10.1109/TBC.2019.2898159.
90. Rahouti M, Xiong K, Xin Y. Secure software-defined networking communication systems for smart cities: current status, challenges, and trends. IEEE Access. 2020;9:12083–113. https://doi.org/10.1109/ACCESS.2020.3047996.
91. Haddad H, Bouyahia Z, Chaudhry SA. A multiagent geosimulation and iot-based framework for safety monitoring in complex dynamic spatial environments. Procedia Computer Sci. 2019;151:527–34. https://doi.org/10.1016/j.procs.2019.04.071.
92. RESIDENTIAL SMART HOME AUTOMATION. KNX Technology and BEMI Automation. [Online]: https://www.bemi.fi/knx-residential-homes/, Last Accessed 20-09-2024

93. Yılmaz Y, Uludağ S, Dilek E, Ayizen Y. A preliminary work on predicting travel times and optimal routes using istanbul's real traffic data. In: 9th Transist Transport Congress and Exhibition (2016)
94. Arshad J, Azad MA, Abdeltaif MM, Salah K. An intrusion detection framework for energy constrained iot devices. Mechanical Syst Signal Process. 2020;136: 106436. https://doi.org/10.1016/j.ymssp.2019.106436.
95. Wirtz BW, Weyerer JC, Schichtel FT. An integrative public iot framework for smart government. Government Inform Quarter. 2019;36(2):333–45. https://doi.org/10.1016/j.giq.2018.07.001.
96. Dalipi E, Abeele F, Ishaq I, Moerman I, Hoebeke J. Ec-iot: An easy configuration framework for constrained iot devices. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE, 2016. https://doi.org/10.1109/wf-iot.2016.7845483 .
97. Mohanty SP, Choppali U, Kougianos E. Everything you wanted to know about smart cities: the internet of things is the backbone. IEEE Consumer Electron Magazine. 2016;5(3):60–70. https://doi.org/10.1109/MCE.2016.2556879.
98. Yaqoob I, Hashem IAT, Ahmed A, Kazmi SA, Hong CS. Internet of things forensics: recent advances, taxonomy, requirements, and open challenges. Future Generat Computer Syst. 2019;92:265–75. https://doi.org/10.1016/j.future.2018.09.058.
99. Xu C, Lin H, Wu Y, Guo X, Lin W. An sdnfv-based ddos defense technology for smart cities. IEEE Access. 2019;7:137856–74. https://doi.org/10.1109/ACCESS.2019.2943146.
100. Lin H, Chen C, Wang J, Qi J, Jin D, Kalbarczyk ZT, Iyer RK. Self-healing attack-resilient pmu network for power system operation. IEEE Trans Smart Grid. 2016;9(3):1551–65. https://doi.org/10.1109/TSG.2016.2593021.
101. Iqbal W, Abbas H, Deng P, Wan J, Rauf B, Abbas Y, Rashid I. Alam: anonymous lightweight authentication mechanism for sdn enabled smart homes. J Netw Computer Appl. 2020;10: 103672.
102. Yu S, Das AK, Park Y. Comments on "alam: anonymous lightweight authentication mechanism for sdn enabled smart homes". IEEE Access. 2021;9:49154–9. https://doi.org/10.1109/ACCESS.2021.3068723.
103. Shirali-Shahreza S, Ganjali Y. Protecting home user devices with an sdn-based firewall. IEEE Trans Consumer Electron. 2018;64(1):92–100. https://doi.org/10.1109/TCE.2018.2811261.
104. Martín-Lopo MM, Boal J, Sánchez-Miralles Á. A literature review of iot energy platforms aimed at end users. Computer Netw. 2020;171: 107101. https://doi.org/10.1016/j.comnet.2020.107101.
105. Liu J, Guo H, Xiong J, Kato N, Zhang J, Zhang Y. Smart and resilient ev charging in sdn-enhanced vehicular edge computing networks. IEEE J Selected Areas Commun. 2019;38(1):217–28. https://doi.org/10.1109/JSAC.2019.2951966.
106. Kaur K, Garg S, Kaddoum G, Ahmed SH, Gagnon F, Atiquzzaman M. Demand-response management using a fleet of electric vehicles: an opportunistic-sdn-based edge-cloud framework for smart grids. IEEE Netw. 2019;33(5):46–53. https://doi.org/10.1109/MNET.001.1800496.
107. Kaur D, Aujla GS, Kumar N, Zomaya AY, Perera C, Ranjan R. Tensor-based big data management scheme for dimensionality reduction problem in smart grid systems: Sdn perspective. IEEE Trans Knowledge Data Eng. 2018;30(10):1985–98. https://doi.org/10.1109/TKDE.2018.2809747.
108. Gui T, Ma C, Wang F, Wilkins DE. Survey on swarm intelligence based routing protocols for wireless sensor networks: An extensive study. In: 2016 IEEE International Conference on Industrial Technology (ICIT). IEEE, 2016. https://doi.org/10.1109/icit.2016.7475064 .
109. Sobhy D, Minku L, Bahsoon R, Chen T, Kazman R. Run-time evaluation of architectures: a case study of diversification in iot. J Syst Softw. 2020;159: 110428. https://doi.org/10.1016/j.jss.2019.110428.
110. Cao T, Xu C, Du J, Li Y, Xiao H, Gong C, Zhong L, Niyato D. Reliable and efficient multimedia service optimization for edge computing-based 5g networks: Game theoretic approaches. IEEE Trans Netw Service Manage. 2020;17(3):1610–25. https://doi.org/10.1109/tnsm.2020.2993886.
111. Boral S. What Happened to Google's Brillo and Weave? iot techtrends. [Online]: https://www.iottechtrends.com/what-happened-google-brillo-weave/, Last Accessed 20-09-2024 2019.
112. Vishwakarma R, Jain AK. A honeypot with machine learning based detection framework for defending iot based botnet ddos attacks. In: 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019. https://doi.org/10.1109/icoei.2019.8862720.
113. Gargenta A. Deep dive into android ipc/binder framework at android builder summit. Marakana Inc. [Online]: https://events.static.linuxfound.org/images/stories/slides/abs2013_gargentas.pdf, Last Accessed 20-09-2024 2013.
114. Vakaloudis A, O'Leary C. A framework for rapid integration of iot systems with industrial environments. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, 2019. https://doi.org/10.1109/wf-iot.2019.8767224 .
115. Thramboulidis K, Vachtsevanou DC, Kontou I. Cpus-iot: a cyber-physical microservice and iot-based framework for manufacturing assembly systems. Ann Rev Control. 2019;47:237–48. https://doi.org/10.1016/j.arcontrol.2019.03.005.
116. Sahil Sood SK. Smart vehicular traffic management: An edge cloud centric iot based framework. Int Things. 2021;14: 100140.
117. Sathwara S, Dutta N, Pricop E. Iot forensic a digital investigation framework for iot systems. In: 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE, 2018. https://doi.org/10.1109/ecai.2018.8679017.
118. Farhan M, Jabbar S, Aslam M, Hammoudeh M, Ahmad M, Khalid S, Khan M, Han K. Iot-based students interaction framework using attention-scoring assessment in elearning. Future Generat Computer Syst. 2018;79:909–19. https://doi.org/10.1016/j.future.2017.09.037.
119. Amazon Aws IoT framework. Amazon AWS. https://aws.amazon.com/iot/, Last Accessed 20-09-2024 (2023)
120. Samsung SmartThings developer documentation. Samsung Electronics. https://developer-preview.smartthings.com/docs/getting-started/welcome/, Last Accessed 20-09-2024 (2023)
121. Ericsson Open source release of IoT app environment calvin. Ericsson. https://www.ericsson.com/, Last Accessed 20-09-2024 (2023)
122. Eclipse Kura framework. Eclipse. https://www.eclipse.org/kura/, Last Accessed 20-09-2024 (2023)
123. Yelmarthi K, Abdelgawad A, Khattab A. An architectural framework for low-power iot applications. In: 2016 28th International Conference on Microelectronics (ICM). IEEE, 2016. https://doi.org/10.1109/icm.2016.7847893 .
124. Khaled AE, Helal S. A framework for inter-thing relationships for programming the social iot. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 2018. https://doi.org/10.1109/wf-iot.2018.8355215 .

125. Nguyen XT, Tran HT, Baraki H, Geihs K. Frasad: A framework for model-driven iot application development. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE, 2015. https://doi.org/10.1109/wf-iot.2015.7389085 .
126. Han Y, Park B, Jeong J. A novel architecture of air pollution measurement platform using 5g and blockchain for industrial iot applications. Procedia Computer Sci. 2019;155:728–33. https://doi.org/10.1016/j.procs.2019.08.105.
127. Pillai AS, Chandraprasad GS, Khwaja AS, Anpalagan A. A service oriented iot architecture for disaster preparedness and forecasting system. Int Things. 2021;14: 100076. https://doi.org/10.1016/j.iot.2019.100076.
128. Lee I. The internet of things for enterprises: an ecosystem, architecture, and iot service business model. Internet of Things. 2019;7: 100078. https://doi.org/10.1016/j.iot.2019.100078.
129. Mocnej J, Seah WKG, Pekar A, Zolotova I. Decentralised iot architecture for efficient resources utilisation. IFAC-PapersOnLine. 2018;51(6):168–73. https://doi.org/10.1016/j.ifacol.2018.07.148.
130. Dawoud A, Shahristani S, Raun C. Deep learning and software-defined networks: towards secure iot architecture. Int Things. 2018;3–4:82–9. https://doi.org/10.1016/j.iot.2018.09.003.
131. Saadeh M, Sleit A, Sabri KE, Almobaideen W. Hierarchical architecture and protocol for mobile object authentication in the context of iot smart cities. J Netw Computer Appl. 2018;121:1–19. https://doi.org/10.1016/j.jnca.2018.07.009.
132. Lee C, Nkenyereye L, Sung N, Song J. Towards a blockchain-enabled iot platform using onem2m standards. In: 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2018. https://doi.org/10.1109/ictc.2018.8539724 .
133. Javed A, Heljanko K, Buda A, Framling K. Cefiot: A fault-tolerant iot architecture for edge and cloud. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 2018. https://doi.org/10.1109/wf-iot.2018.8355149 .
134. Kum SW, Moon J, Lim T-B. Design of fog computing based iot application architecture. In: 2017 IEEE 7th International Conference on Consumer Electronics - Berlin (ICCE-Berlin). IEEE, 2017. https://doi.org/10.1109/icce-berlin.2017.8210598 .
135. Wang S, Hou Y, Gao F, Ji X. A novel iot access architecture for vehicle monitoring system. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE, 2016. https://doi.org/10.1109/wf-iot.2016.7845396 .
136. Park H, Kim H, Joo H, Song J. Recent advancements in the internet-of-things related standards: a onem2m perspective. ICT Express. 2016;2(3):126–9. https://doi.org/10.1016/j.icte.2016.08.009.
137. Hudda S, Haribabu K, Barnwal R. A novel approach for energy-efficient communication in a constrained iot environment. In: 2024 International Conference on Information Networking (ICOIN), pp. 699–704 2024. https://doi.org/10.1109/ICOIN59985.2024.10572211 . IEEE.
138. Hudda S, Haribabu K, Balani V. An energy efficient data transmission approach in smart iot systems. In: 2024 International Conference on Information Networking (ICOIN), pp. 740–745 2024. https://doi.org/10.1109/ICOIN59985.2024.10572103 . IEEE.
139. Li C, Ye M, Chen G, Wu J. An energy-efficient unequal clustering mechanism for wireless sensor networks. In: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, p. 8. IEEE, 2005. https://doi.org/10.1109/mahss.2005.1542849 .
140. Liu P, Huang T-l, Zhou X-y, Wu G-x: An improved energy efficient unequal clustering algorithm of wireless sensor network. In: 2010 International Conference on Intelligent Computing and Integrated Systems, pp. 930–933. IEEE, 2010. https://doi.org/10.1109/iciss.2010.5657032 .
141. Bagci H, Yazici A. An energy aware fuzzy unequal clustering algorithm for wireless sensor networks. In: International Conference on Fuzzy Systems, pp. 1–8. IEEE, 2010. https://doi.org/10.1109/FUZZY.2010.5584580 .
142. Baranidharan B, Santhi B. Ducf: distributed load balancing unequal clustering in wireless sensor networks using fuzzy approach. Appl Soft Comput. 2016;40:495–506. https://doi.org/10.1016/j.asoc.2015.11.044.
143. Zhang R, Ju L, Jia Z, Li X. Energy efficient routing algorithm for wsns via unequal clustering. In: 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems, pp. 1226–1231. IEEE, 2012. https://doi.org/10.1109/HPCC.2012.180 .
144. Logambigai R, Kannan A. Fuzzy logic based unequal clustering for wireless sensor networks. Wireless Netw. 2016;22:945–57. https://doi.org/10.1007/s11276-015-1013-1.
145. Zhang D-G, Liu S, Zhang T, Liang Z. Novel unequal clustering routing protocol considering energy balancing based on network partition & distance for mobile education. J Netw Computer Appl. 2017;88:1–9. https://doi.org/10.1016/j.jnca.2017.03.025.
146. Hamidzadeh J, Ghomanjani MH. An unequal cluster-radius approach based on node density in clustering for wireless sensor networks. Wireless Personal Commun. 2018;101(3):1619–37. https://doi.org/10.1007/s11277-018-5779-1.
147. Gajjar S, Sarkar M, Dasgupta K. Famacrow: fuzzy and ant colony optimization based combined mac, routing, and unequal clustering cross-layer protocol for wireless sensor networks. Applied Soft Comput. 2016;43:235–47. https://doi.org/10.1016/j.asoc.2016.02.019.
148. Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, p. 10. IEEE Comput. Soc, 2000. https://doi.org/10.1109/hicss.2000.926982 .
149. Al-Shaikh A, Khattab H, Al-Sharaeh S. Performance comparison of leach and leach-c protocols in wireless sensor networks. J ICT Res Appl. 2018;12(3):219–36. https://doi.org/10.5614/itbj.ict.res.appl.2018.12.3.2.
150. Chakraborty UK, Das SK, Abbott TE. Energy-efficient routing in hierarchical wireless sensor networks using differential-evolution-based memetic algorithm. In: 2012 IEEE Congress on Evolutionary Computation. IEEE, 2012. https://doi.org/10.1109/cec.2012.6252985 .
151. Singh K, Kaur J. Machine learning based link cost estimation for routing optimization in wireless sensor networks. Adv Wireless Mobile Commun. 2017;10(1):39–50.
152. Ali B, Mahmood T, Abbas M, Hussain M, Ullah H, Sarker A, Khan A. Leach robust routing approach applying machine learning. IJCSNS Int J Computer Sci Netw Security. 2019;19(6):18–26.
153. Nehra NK, Kumar M, Patel R. Neural network based energy efficient clustering and routing in wireless sensor networks. In: 2009 First International Conference on Networks & Communications, pp. 34–39. IEEE, 2009. https://doi.org/10.1109/NetCoM.2009.56 .

154. Bin G, Zhe L, Ze-Jun W. A dynamic-cluster energy-aware routing algorithm based on neural structure in the wireless sensor networks. In: The Fifth International Conference on Computer and Information Technology (CIT'05), pp. 401–405. IEEE, 2005. https://doi.org/10.1109/CIT.2005.8 .
155. Zhao W, Liu D, Jiang Y. Distributed neural network routing algorithm based on global information of wireless sensor network. In: 2009 WRI International Conference on Communications and Mobile Computing. IEEE, 2009. https://doi.org/10.1109/cmc.2009.103 .
156. Arabi Z. Herf: A hybrid energy efficient routing using a fuzzy method in wireless sensor networks. In: 2010 International Conference on Intelligent and Advanced Systems, pp. 1–6. IEEE, 2010. https://doi.org/10.1109/ICIAS.2010.5716145 .
157. Jaradat T, Benhaddou D, Balakrishnan M, Al-Fuqaha A. Energy efficient cross-layer routing protocol in wireless sensor networks based on fuzzy logic. In: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 177–182. IEEE, 2013. https://doi.org/10.1109/iwcmc.2013.6583555 .
158. Venkataramana S, Sekhar BVDS, Deshai N, Chakravarthy VVSSS, Krishna Rao S. Efficient time reducing and energy saving routing algorithm for wireless sensor network. J Phys Conf Series. 2019;1228(1): 012002. https://doi.org/10.1088/1742-6596/1228/1/012002.
159. Li J, Li Y, Ren J, Wu J. Hop-by-hop message authentication and source privacy in wireless sensor networks. IEEE Trans Parallel Distr Syst. 2014;25(5):1223–32. https://doi.org/10.1109/tpds.2013.119.
160. Luo S, Wu J, Li J, Guo L. A multi-stage attack mitigation mechanism for software-defined home networks. IEEE Trans Consumer Electron. 2016;62(2):200–7. https://doi.org/10.1109/TCE.2016.7514720.
161. Lee H, Kang D, Ryu J, Won D, Kim H, Lee Y. A three-factor anonymous user authentication scheme for internet of things environments. J Inform Secur Appl. 2020;52: 102494. https://doi.org/10.1016/j.jisa.2020.102494.
162. Ali G, Ahmad N, Cao Y, Khan S, Cruickshank H, Qazi EA, Ali A. xdbauth: Blockchain based cross domain authentication and authorization framework for internet of things. IEEE Access. 2020;8:58800–16. https://doi.org/10.1109/access.2020.2982542.
163. Ferrag MA, Maglaras L, Ahmim A, Derdour M, Janicke H. Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. Future Int. 2020;12(3):44. https://doi.org/10.3390/fi12030044.
164. Anthi E, Williams L, Slowinska M, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home iot devices. IEEE Int Things J. 2019;6(5):9042–53. https://doi.org/10.1109/jiot.2019.2926365.
165. Sforzin A, Marmol FG, Conti M, Bohli J-M. Rpids: Raspberry pi ids - a fruitful intrusion detection system for iot. In: 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld). IEEE, 2016. https://doi.org/10.1109/uic-atc-scalcom-cbdcom-iop-smartworld.2016.0080
166. Ahmim A, Derdour M, Ferrag MA. An intrusion detection system based on combining probability predictions of a tree of classifiers. International Journal of Communication Systems 2018;31(9). https://doi.org/10.1002/dac.3547
167. Li F, Shi Y, Shinde A, Ye J, Song W. Enhanced cyber-physical security in internet of things through energy auditing. IEEE Int Things J. 2019;6(3):5224–31. https://doi.org/10.1109/jiot.2019.2899492.
168. Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M. Design of secure user authenticated key management protocol for generic iot networks. IEEE Int Things J. 2018;5(1):269–82. https://doi.org/10.1109/jiot.2017.2780232.
169. Esposito C, Ficco M, Castiglione A, Palmieri F, De Santis A. Distributed group key management for event notification confidentiality among sensors. IEEE Transactions on Dependable and Secure Computing, 1–1 2019. https://doi.org/10.1109/tdsc.2018.2799227