Soft Computing Fusion with Applications

www.scfa.reapress.com

Soft. Comput. Fusion. Appl. Vol. 2, No. 1 (2025) 164–184.

Paper Type: Original Article

Securing the Future: AI-Driven Data Transmission in IoT-Powered Smart Cities

Aurgho Banerjee*

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 2229022@kiit.ac.in.

Citation:

Received: 15 July 2024 *Revised: 10 September 2024* *Accepted: 25 February 2025*	Banerjee, A. (2025). Securing the future: AI-driven data transmission in IoT-powered smart cities. *Soft computing fusion with applications, 2*(1), 164-184.

Abstract

The swift adoption of Artificial Intelligence (AI) alongside the Internet of Things (IoT) has revolutionized smart cities, allowing for improved urban services such as traffic control, energy management, healthcare delivery, and public safety. However, the extensive generation and transmission of sensitive data by IoT devices present substantial cybersecurity risks. Unprotected data transmission can result in privacy violations, unauthorized access, and vulnerabilities within systems, jeopardizing the integrity and efficiency of smart city frameworks. This paper investigates the essential elements of secure data transmission within AI-driven IoT networks. It analyzes different encryption techniques, AI-enhanced Intrusion Detection Systems (IDSs), and decentralized frameworks based on blockchain to guarantee data integrity and confidentiality. Moreover, we emphasize the importance of federated learning, which enables distributed AI models to enhance their performance while keeping sensitive information localized, thereby reducing the likelihood of data breaches. Significant challenges are addressed, including the computational constraints of IoT devices, the diversity of IoT networks, and the requirement for low-latency communication in real-time scenarios. Innovative solutions, such as quantum-resistant cryptography and the potential of 6G technology, are also examined. The paper concludes by outlining future research and development pathways aimed at improving the security, scalability, and efficiency of IoT networks within smart cities.

Keywords: Smart cities, Artificial intelligence-enabled internet of things, Secure data transmission, Blockchain, Federated learning.

1 | Introduction

Smart cities have emerged as a solution to the growing challenges of urbanization, population growth, and resource management. Smart cities leverage technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) to enhance the efficiency and sustainability of urban services, including transportation,

Corresponding Author: 2229022@kiit.ac.in

healthcare, energy, and public safety [1], [2]. By deploying interconnected sensors, devices, and communication networks, smart cities are designed to optimize various aspects of daily life, enabling better resource allocation, reducing congestion, improving public health, and increasing overall quality of life.

IoT devices are at the heart of this transformation, which collects vast amounts of real-time data from various sources across the urban environment. These devices include traffic sensors and smart meters, healthcare wearables, and environmental monitors. AI algorithms process this data, providing insights that facilitate automated decision-making and predictive analytics. For instance, AI can predict traffic patterns, adjust energy distribution, monitor air quality, and even provide personalized healthcare solutions [3], [4]. However, as the volume of data grows, so do the concerns surrounding its security and privacy [5], [6].

Data transmission between IoT devices and central processing units, such as cloud servers or edge computing nodes, plays a critical role in the functioning of smart city systems [7], [8]. The real-time nature of these transmissions means that any delay, interruption, or manipulation can have severe consequences. For example, a cyber attack targeting traffic control systems could lead to accidents, while a breach in healthcare systems could expose sensitive patient information [9]. The stakes are high, as these attacks not only disrupt services but can also undermine trust in the smart city infrastructure.

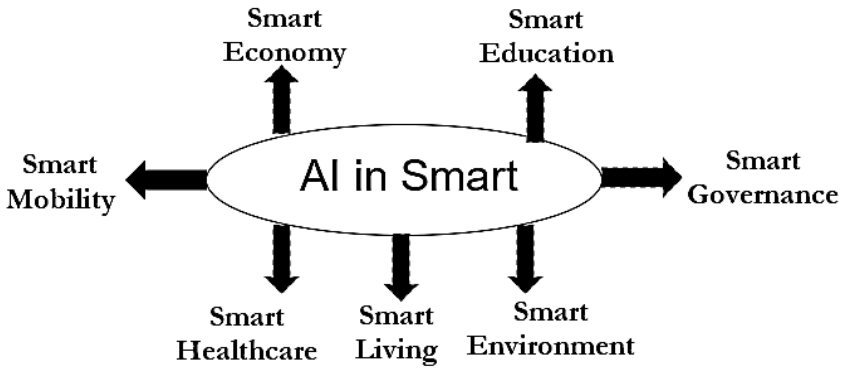

Fig.1. Sustainable development goals.

1.1 | Importance of Secure Data Transmission

The security of data transmission in AI-enabled IoT networks is a critical aspect that cannot be overlooked. Data flows through multiple layers, starting from IoT devices, moving to communication networks, and eventually reaching AI systems for analysis. At each stage, there are potential vulnerabilities that malicious actors can exploit.

Confidentiality: IoT devices often handle sensitive data, such as personal health records or financial transactions, which must be kept confidential. Unauthorized access to this data can lead to privacy violations, identity theft, or financial fraud.

Integrity: ensuring the accuracy and completeness of data during transmission is essential. Any tampering or data corruption could lead to incorrect decisions by AI systems, potentially causing service failures or harmful outcomes.

Availability: smart city services rely on continuous, real-time data transmission. Denial-of-service (DoS) attacks or network failures can disrupt the availability of critical services, such as emergency response systems or smart grids.

Given these challenges, secure data transmission is paramount to the success and sustainability of smart cities. While effective, traditional security solutions, such as encryption, may not be sufficient in the highly dynamic and resource-constrained environments of IoT networks. This is especially true given the increasing sophistication of cyber threats, which can bypass conventional defenses. Moreover, many IoT devices are

resource-limited in processing power, memory, and energy, making it difficult to implement robust security protocols without affecting performance [10].

1.2 | Role of Artificial Intelligence in Enhancing Internet of Things Security

AI plays a dual role in smart cities: not only does it optimize city services, but it also enhances the security of the underlying IoT networks [11]. By leveraging Machine Learning (ML) algorithms, AI can detect anomalies in network traffic, identify potential cyber-attacks in real-time, and even predict future threats based on historical data [12]. AI-driven security systems, such as Intrusion Detection Systems (IDSs) [13], can automatically adapt to new attacks, providing a more dynamic and responsive approach to cybersecurity than traditional rule-based systems.

Moreover, AI can be integrated into encryption algorithms to enhance efficiency and strength. For example, AI can optimize key management protocols, identify real-time vulnerabilities, and ensure that data remains protected even during a network breach. With advanced techniques like federated learning [14], AI can enable secure, decentralized data analysis, allowing IoT devices to contribute to AI model training without sharing sensitive raw data.

1.3 | Research Objectives and Structure

This paper explores the security challenges and solutions for data transmission in AI-enabled IoT networks within smart cities. It aims to provide an in-depth analysis of various security techniques, including encryption, AI-driven intrusion detection, blockchain-based authentication, and federated learning. By examining these methods, the paper identifies the current limitations and possibilities for securing smart city infrastructures.

The rest of the paper is structured as follows:

Section 2 provides an overview of AI-enabled IoT networks, including their components and communication protocols.

Section 3 discusses the challenges of secure data transmission in IoT environments.

Section 4 explores solutions for securing data transmission, including encryption, AI-driven IDS, and blockchain technology.

Section 5 presents case studies that illustrate the practical applications of these solutions in real-world smart city deployments.

Section 6 examines emerging technologies and future directions for secure IoT communication, including quantum-resistant cryptography and the potential of 6G networks.

Section 7 concludes the paper by summarizing the key findings and suggesting avenues for future research. By addressing the complexities of secure data transmission in AI-enabled IoT networks, this paper contributes to developing resilient and secure smart city infrastructures that can withstand evolving cyber threats.

2 | Overview of Artificial Intelligence-Enabled Internet of Things Networks

Integrating AI with the IoT has given rise to AI-enabled IoT networks, which form the backbone of smart city infrastructures [15]. These networks consist of interconnected devices that collect, process, and transmit data in real time. AI is pivotal in analyzing this data, enabling automated decision-making, predictive maintenance, and optimizing urban services such as energy management, traffic control, and public safety.

In this section, we will explore the key components of AI-enabled IoT networks, the communication protocols that enable them, and the challenges they face in the context of smart cities.

2.1 | Components of Artificial Intelligence-Enabled Internet of Things Networks

AI-enabled IoT networks comprise several interconnected layers, each performing specific functions to support smart city applications. These layers include IoT devices, communication networks, AI models, and cloud/edge computing infrastructure.

2.1.1 | Internet of things devices

IoT devices are the fundamental building blocks of any AI-enabled IoT network. These devices have sensors, actuators, and communication modules to collect and transmit real-time data.

Examples of IoT devices in smart cities include:

I. Environmental sensors: devices that monitor air quality, temperature, humidity, and pollution levels [16].

II. Smart meters: sensors that track energy and water consumption in residential and commercial buildings [17].

III. Traffic sensors monitor vehicle flow, congestion, and traffic patterns [18].

IV. Healthcare wearables: wearable devices that collect biometric data such as heart rate, blood pressure, and oxygen levels for patient monitoring [19].

V. Smart lighting and waste management systems are devices that optimize energy usage for streetlights and automate waste collection processes based on bin capacity [20].

These IoT devices generate enormous amounts of raw data that must be transmitted and processed efficiently to support real-time decision-making in smart city environments. Since these devices are often resource-constrained in terms of power, memory, and processing capacity, ensuring secure data transmission is critical without compromising performance.

2.1.2 | Communication protocols

IoT devices rely on various communication protocols to transmit data between each other and central processing systems. The protocol choice depends on distance, data rate, power consumption, and network topology.

In AI-enabled IoT networks, several common protocols are used, including:

I. Wi-Fi: widely used for short-range, high-bandwidth communication in urban areas. Wi-Fi is often used in smart homes, public transportation systems, and buildings [21].

II. 5G: the next generation of cellular communication, 5G offers ultra-low latency and high-speed data transmission [22]. It is expected to be a key enabler of AI-driven smart city applications, such as Autonomous Vehicles (AVs) and smart healthcare.

III. LoRaWAN: a Low-Power, Wide-Area Network (LPWAN) protocol, LoRaWAN is ideal for long-range communication with minimal power consumption [23]. It is commonly used in smart meters and environmental monitoring systems.

IV. Bluetooth Low Energy (BLE) is a low-power, short-range communication protocol often used in wearable devices and smart health applications [24].

V. Zigbee is another low-power protocol designed for short-range communication. It is widely used in home automation systems and smart lighting solutions [25].

These protocols enable IoT devices to transmit data efficiently but also introduce potential vulnerabilities, such as unauthorized access or data interception during transmission.

2.1.3 | Artificial intelligence algorithms

AI algorithms form the intelligence layer of IoT networks, enabling data analysis, decision-making, and automation. In smart cities, AI processes the vast amounts of data IoT devices generate to derive real-time actionable insights. There are several types of AI algorithms used in IoT networks.

I. ML: ML models are trained to identify patterns in data, enabling predictive analytics. For example, ML models can predict traffic congestion or energy demand based on historical data [26].

II. Deep Learning (DL): a subset of ML, DL uses neural networks to process complex, high-dimensional data [27]. DL is used in applications such as computer vision (e.g., surveillance cameras in smart cities) and natural language processing (e.g., voice-activated smart assistants) [28].

III. Reinforcement Learning (RL): RL models are used for decision-making in dynamic environments. For instance, RL can optimize traffic signals in response to real-time traffic conditions [29].

AI algorithms continuously improve their accuracy and performance by learning from new data. In smart city contexts, these models automate urban services such as traffic control, waste management, and energy distribution.

2.1.4 | Cloud and edge computing

AI-enabled IoT networks rely on a combination of cloud and edge computing infrastructure to process and store data. Cloud computing offers centralized processing power and storage, allowing large-scale AI models to analyze data from multiple IoT devices across the city [30]. However, cloud computing can introduce latency, which is problematic for applications that require real-time decision-making.

Edge computing addresses this issue by processing data closer to the source, i.e., at the network's edge, on IoT devices or local servers. By reducing the need to transmit all data to the cloud, edge computing minimizes latency and allows for faster responses. In smart cities, edge computing is used in applications such as AVs, real-time surveillance, and emergency response systems.

2.2 | Security Concerns in Artificial Intelligence-Enabled Internet of Things Networks

While AI-enabled IoT networks offer significant benefits for smart cities, they also introduce new security challenges. The interconnected nature of IoT devices, combined with the massive volume of data generated, makes these networks attractive targets for cyber attacks [31]. Some of the key security concerns include:

2.2.1 | Data interception and eavesdropping

Data transmitted between IoT devices and central processing systems is vulnerable to interception by unauthorized actors. This is especially concerning in smart cities where sensitive data, such as personal health records or financial transactions, is often transmitted. Without proper encryption, this data can be easily accessed and misused.

2.2.2 | Unauthorized device access

IoT devices deployed in smart cities are often physically accessible, making them susceptible to tampering or unauthorized control. Attackers could hijack IoT devices to manipulate their behavior, disrupt services, or gain access to sensitive data. For example, an attacker could take control of traffic lights to create congestion or accidents.

2.2.3 | Network intrusion and malware attacks

Hackers can exploit vulnerabilities in IoT devices or communication protocols to infiltrate the network and install malware. Once inside the network, attackers can steal data, disrupt services, or launch Distributed

Denial-of-Service (DDoS) attacks that overwhelm the system and cause downtime. AI-driven IoT systems are particularly vulnerable to these attacks, relying heavily on continuous data streams to function effectively.

2.2.4 | Privacy violations

Smart city applications often involve collecting and analyzing personal data, such as location, health, and financial information. If this data is not properly secured, it could be exposed, leading to privacy violations and legal repercussions. AI algorithms to process this data must be designed with privacy in mind, ensuring that sensitive information is protected and anonymized.

2.3 | Challenges in Securing Artificial Intelligence-Enabled Internet of Things Networks

Securing AI-enabled IoT networks in smart cities presents several challenges:

I. Resource constraints: many IoT devices have limited computational power, memory, and battery life, making it difficult to implement robust security measures, such as encryption and authentication protocols.

II. Heterogeneous networks: smart cities have various IoT devices using different communication protocols and standards. This heterogeneity complicates the implementation of a unified security framework that can protect all devices and data.

III. Real-time processing requirements: many smart city applications, such as traffic control and emergency response, require real-time data processing and communication. Introducing security measures that cause delays or increase latency can negatively impact the performance of these critical systems.

2.4 | The Role of Artificial Intelligence in Enhancing Internet of Things Security

AI enables smart city applications and plays a crucial role in securing IoT networks. AI-driven security systems, such as IDS, use ML algorithms to monitor network traffic, detect anomalies, and identify potential threats. These systems can adapt to new attacks in real time, providing a more dynamic and responsive defense than traditional security solutions.

AI can also enhance encryption techniques, optimize key management processes, and ensure data remains protected throughout its lifecycle. With the advent of federated learning, AI models can be trained across multiple devices without sharing raw data, reducing the risk of data breaches and enhancing privacy.

3 | Challenges in Securing Data Transmission in Artificial Intelligence-Internet of Things Networks

As AI-enabled IoT networks play an increasingly crucial role in smart city infrastructure, ensuring data transmission security becomes essential to maintaining the integrity, availability, and confidentiality of smart city services. However, securing data transmission in these networks presents a wide range of challenges due to the inherent characteristics of IoT devices, their communication protocols, and the urban environments in which they operate. This section discusses the major challenges in securing data transmission in AI-enabled IoT networks, focusing on resource constraints, heterogeneity, latency requirements, scalability, and evolving cyber threats.

3.1 | Resource Constraints of Internet of Things Devices

One of the most significant challenges in securing data transmission in IoT networks is the resource-constrained nature of IoT devices [32]. These devices are designed to be low-power, low-cost, and compact, with limited computational capabilities, memory, and energy supply. These constraints limit the ability of IoT devices to implement traditional, computationally intensive security measures, such as strong encryption algorithms and authentication protocols.

I. Limited processing power: IoT devices often lack the processing power to execute advanced encryption algorithms or perform real-time cryptographic operations. While strong encryption protocols like Advanced Encryption Standard (AES)-256 provide robust data protection, they require significant processing resources that many IoT devices, such as sensors and wearables, do not have.

II. Battery limitations: many IoT devices, especially those deployed in remote or inaccessible areas, rely on batteries for power. Implementing security mechanisms like encryption, authentication, and frequent key exchanges consumes additional energy, shortening the device's operational lifespan. Balancing security with energy efficiency is a key challenge in ensuring secure data transmission without draining the device's battery.

III. Memory constraints: IoT devices have limited memory capacity, which restricts their ability to store large security libraries or encryption keys. Devices may be unable to support advanced security features, such as complex Public Key Infrastructure (PKI) systems, without running out of memory resources.

To address these constraints, lightweight security solutions must be developed that provide adequate protection while minimizing the computational and energy overhead. Lightweight encryption algorithms like Elliptic Curve Cryptography (ECC) and optimized hashing functions aim to reduce resource consumption while maintaining data security.

3.2 | Heterogeneity of Internet of Things Networks

AI-enabled IoT networks are highly heterogeneous, consisting of various devices, sensors, communication protocols, and architectures. This diversity complicates the implementation of standardized security measures across the entire network.

Diverse communication protocols: IoT devices in smart cities use a range of communication protocols, including Wi-Fi, Bluetooth, LoRaWAN, Zigbee, and 5G. Each protocol has its security features, vulnerabilities, and performance characteristics. For example, Zigbee and Bluetooth are designed for low-power, short-range communication and may not support advanced security mechanisms like 5G. Ensuring consistent security across these protocols is challenging, as they may not be interoperable or require different levels of encryption and authentication.

Varied device capabilities: IoT networks include devices with varying levels of computational power and security support. For instance, a smart traffic light may have more resources available for security than a tiny environmental sensor. Designing security protocols that can be applied across all devices in the network, regardless of their capabilities, is difficult. The weakest device in the network can become a potential entry point for attackers, compromising the entire system.

Interoperability issues: IoT networks often need to integrate devices from multiple manufacturers, each with proprietary security solutions. Lack of standardization and interoperability between devices and protocols can lead to security gaps. When devices from different vendors are used, their security policies may be inconsistent or incompatible, making it difficult to create a unified, secure network architecture.

A solution to this challenge involves developing flexible security frameworks that can adapt to different devices and protocols' specific needs and capabilities. Adaptive encryption techniques and security standards, such as IEEE 802.1X, can help create a more consistent and interoperable security framework for heterogeneous IoT networks.

3.3 | Real-Time Data Transmission and Low Latency Requirements

Many AI-enabled IoT applications in smart cities require real-time data transmission and low-latency communication to function effectively. Services such as traffic management, AVs, emergency response systems, and smart grid operations demand that data be transmitted, processed, and acted upon almost instantaneously. However, introducing security measures, such as encryption and authentication, can introduce delays in data transmission, negatively impacting the performance of time-sensitive applications.

Encryption overhead: encrypting and decrypting data adds processing time, especially for resource-constrained IoT devices. This can lead to increased latency in data transmission, which is unacceptable for applications like AVs, where even milliseconds of delay can result in accidents.

Authentication delays: implementing strong authentication mechanisms, such as PKI, can also introduce delays in verifying the identity of devices and users. For example, Public-Key cryptography often requires several rounds of communication to establish a secure session, which can slow down data transmission in latency-sensitive environments.

Communication bottlenecks: in smart cities, IoT devices generate massive amounts of data, which must be transmitted through communication networks that can become congested or experience delays. Security measures that involve additional data transmission, such as key exchanges or re-encryption of data packets, can exacerbate these communication bottlenecks.

To address this challenge, new security techniques must be developed to minimize the impact of latency while maintaining strong data protection. Edge computing, where data is processed closer to its source (on the network's edge), is one approach to reducing latency and enabling real-time, secure data transmission.

3.4 | Scalability and Large-Scale Deployment

The scale of AI-enabled IoT networks in smart cities is vast, with potentially millions of interconnected devices generating and transmitting data. Securing data transmission in large-scale deployments presents several challenges, including key management, monitoring, and system updates.

Key management complexity: when keys must be updated regularly to prevent compromise, managing encryption keys for many IoT devices is complex. Traditional key management solutions involving central servers or trusted third parties can become bottlenecks in large-scale IoT deployments. Additionally, securely distributing keys to millions of devices is a logistical challenge, particularly when devices may not have continuous connectivity.

Monitoring and intrusion detection: monitoring the security of data transmission in large-scale IoT networks is daunting. With such a high volume of data and devices, identifying anomalies or detecting potential intrusions becomes more difficult. Traditional IDS may struggle to keep up with the scale of data generated by smart cities, leading to delayed detection of attacks or an increased number of false positives.

System updates and patches: IoT devices in smart cities require regular software updates to patch security vulnerabilities and improve functionality. However, deploying these updates at scale can be challenging, particularly for devices with limited connectivity or those deployed in remote or difficult-to-access areas. Delayed or incomplete device patching can leave the network vulnerable to cyber attacks.

Scalable security solutions, such as blockchain-based distributed key management systems and AI-driven intrusion detection, are being explored to address these challenges. Blockchain technology, for instance, can provide a decentralized, tamper-proof ledger for managing encryption keys and authentication records across large-scale IoT networks.

3.5 | Evolving Cyber Threats and Zero-Day Vulnerabilities

The rapidly evolving landscape of cyber threats presents an ongoing challenge in securing data transmission in AI-enabled IoT networks. Attackers continuously develop new methods to exploit vulnerabilities in IoT devices, communication protocols, and AI algorithms. Some of the key threats include:

I. Zero-day vulnerabilities: a zero-day vulnerability is a security flaw that is unknown to the software or hardware vendor and, therefore, unpatched. Attackers exploit these vulnerabilities before the vendor can develop a fix, potentially compromising IoT devices or AI models. In large-scale IoT networks, detecting and responding to zero-day attacks is particularly challenging due to the wide attack surface and the interconnected nature of devices.

II. Man-in-the-Middle (MITM) attacks: in a MITM attack, an attacker intercepts data transmitted between IoT devices and central servers, potentially altering or eavesdropping the data. IoT devices are particularly vulnerable to these attacks without strong encryption and authentication.

III. AI algorithm manipulation: as AI plays a central role in analyzing data and making decisions in smart cities, attackers may attempt to manipulate AI algorithms by injecting malicious data or exploiting weaknesses in the training process. For example, attackers could poison training data to cause AI models to make incorrect predictions, such as misidentifying traffic patterns or mismanaging energy distribution.

IoT networks must implement adaptive security solutions to respond to new attack vectors in real-time to combat these evolving threats. AI-driven security systems, such as anomaly detection and behavioral analysis, can help identify and mitigate emerging threats before they cause significant damage.

4 | Solutions for Secure Data Transmission in Artificial Intelligence-Internet of Things Networks

Several innovative solutions have been developed to address the challenges in securing data transmission in AI-enabled IoT networks. These solutions focus on optimizing security without compromising performance. These solutions leverage lightweight encryption, decentralized key management, AI-based anomaly detection, and secure hardware to provide comprehensive protection for IoT devices in smart city environments.

4.1 | Lightweight Cryptography for Internet of Things Devices

Since IoT devices are often resource-constrained, traditional cryptographic techniques, such as AES or RSA, are too computationally heavy to implement efficiently. As a result, lightweight cryptographic algorithms have been developed specifically for IoT devices to provide secure data transmission with minimal resource consumption.

4.1.1 | Elliptic curve cryptography

ECC is a highly efficient public-key encryption method that provides equivalent security to RSA but requires much shorter key lengths. This makes ECC ideal for IoT devices with limited processing power and memory. ECC enables secure data transmission by encrypting data and allowing secure key exchanges between devices with minimal computational overhead. Its smaller key size reduces storage requirements and transmission bandwidth, making it a lightweight yet secure solution.

4.1.2 | Lightweight encryption algorithms

Specialized lightweight encryption algorithms, such as PRESENT, CLEFIA, and SPECK, have been designed to reduce encryption processes' computational and energy demands. These algorithms provide sufficient security for IoT data transmission while consuming significantly less power and processing resources than traditional cryptographic methods. PRESENT, for example, is a block cipher with a simple structure that can be implemented in hardware or software. It is particularly well-suited for IoT devices with low power and memory capacities.

4.2 | Secure Communication Protocols

Communication protocols play a vital role in IoT data transmission, and securing these protocols is essential to prevent attacks such as eavesdropping and tampering. Several secure protocols and mechanisms have been developed to enhance the security of data transmission in IoT networks.

4.2.1 | Datagram transport layer security

Datagram Transport Layer Security (DTLS) is a protocol designed to provide encryption, integrity, and authentication for datagram-based communication, which is common in IoT networks. As a variant of Transport Layer Security (TLS), DTLS ensures that data transmitted over connectionless protocols, such as

UDP, is encrypted and protected against tampering. DTLS is ideal for IoT applications, including smart meters and environmental sensors, where real-time, low-latency communication is required.

4.2.2 | Lightweight secure shell

Lightweight Secure Shell (LwSSH) is a streamlined version of the Secure Shell (SSH) protocol, optimized for resource-constrained IoT devices. LwSSH provides secure, encrypted channels for communication between IoT devices and servers, ensuring that transmitted data is protected from unauthorized access or tampering. It is particularly useful for securing communications where IoT devices must establish remote sessions with cloud servers or other central systems.

4.3 | Decentralized Key Management

Traditional key management systems rely on centralized authorities to generate and distribute encryption keys, which can become bottlenecks in large-scale IoT networks. Moreover, central key management systems are vulnerable to single points of failure. Decentralized key management systems provide a more scalable and resilient approach to managing encryption keys across distributed IoT networks.

4.3.1 | Blockchain-based key management

Blockchain technology offers a decentralized and tamper-resistant approach to managing encryption keys in large-scale IoT networks. In a blockchain-based key management system, encryption keys are securely distributed and verified through the blockchain's consensus mechanism, ensuring that no single entity controls the key management process. This approach prevents key compromise and enhances transparency and accountability in the network.

Blockchain-based systems can be used in AI-enabled IoT networks, including secure device registration, authentication, and encrypted data transmission. For instance, blockchain can create secure, immutable logs of key exchanges, ensuring that encryption keys remain valid and uncompromised.

4.3.2 | Identity-based encryption

Identity-based encryption (IBE) is a public-key cryptosystem in which a device's public key is derived from its unique identity (e.g., device ID, email address) rather than from a central key management authority. IBE eliminates the need for pre-distributed certificates or PKI, making it easier to manage encryption keys in large-scale IoT networks. Using device identities to generate encryption keys, IBE simplifies the key distribution process and reduces reliance on centralized authorities.

4.4 | Artificial Intelligence-Based Anomaly Detection and Intrusion Prevention

AI-enabled IoT networks benefit from AI-based security mechanisms that detect anomalies and prevent real-time cyberattacks. These systems leverage ML and DL algorithms to identify patterns in network traffic and device behavior, enabling rapid detection of suspicious activities.

4.4.1 | Machine learning for intrusion detection

ML algorithms can monitor network traffic and detect anomalous patterns that may indicate a potential attack, such as unusual data transmission rates, unexpected device behavior, or unauthorized access attempts. AI-based IDS continuously learn from historical data and adapt to new attack patterns, enabling them to identify and mitigate emerging threats more effectively than traditional rule-based systems.

For example, a smart city's traffic management system can use ML models to detect anomalies in traffic sensor data that may indicate tampering or unauthorized access. By detecting these anomalies early, the system can prevent further damage and ensure the integrity of the transmitted data.

4.4.2 | Federated learning for distributed security

Federated learning is an advanced AI technique where AI models are trained across multiple devices without sharing raw data. Instead of transmitting sensitive data to a central server for processing, each IoT device updates the global AI model locally, using its data. These updates are then aggregated to improve the overall model without compromising privacy or security.

Federated learning is particularly useful in securing IoT networks. It enables AI-driven security solutions (such as anomaly detection or intrusion prevention) to be implemented across devices without exposing sensitive data to external networks. It reduces the risk of data breaches while ensuring that AI models are continuously improved based on local data.

4.5 | Secure Hardware Solutions

In addition to software-based security mechanisms, secure hardware components are essential for protecting IoT devices from physical tampering and ensuring the integrity of data transmission.

4.5.1 | Trusted platform module

A Trusted Platform Module (TPM) is a secure hardware component that provides a trusted environment for cryptographic operations. TPMs can generate, store, and manage encryption keys securely, ensuring that sensitive keys are not exposed to external threats. TPMs also support secure boot processes, ensuring IoT devices start in a known, trusted state. By integrating TPMs into IoT devices, manufacturers can enhance the security of data transmission and prevent tampering or unauthorized access to encryption keys [33].

4.5.2 | Hardware security modules

Hardware Security Modules (HSMs) are specialized hardware devices designed to perform cryptographic operations securely. HSMs are used to offload encryption, decryption, and key management tasks from IoT devices to dedicated hardware components that are resistant to tampering. HSMs can be deployed in cloud or edge environments to manage encryption keys and secure data transmission across large IoT networks.

Using HSMs, IoT networks can ensure that cryptographic operations are performed in a highly secure environment, reducing the risk of key compromise and enhancing the overall security of data transmission.

4.6 | Secure Edge Computing

Edge computing helps reduce latency in IoT networks by processing data closer to its source (on edge devices) rather than transmitting all data to the cloud. Secure edge computing enhances this model by ensuring that data is encrypted and processed securely at the edge, reducing the risk of interception or tampering during transmission.

4.6.1 | Data encryption at the edge

Edge devices can encrypt data locally before transmitting it to central servers, ensuring that sensitive information remains protected. By applying encryption at the edge, even if an attacker intercepts data during transmission, the information remains unreadable without the correct decryption key.

4.6.2 | Secure edge analytics

AI-driven analytics can be performed on edge devices to process and analyze data securely in real time. For instance, edge devices can securely analyze energy consumption data in a smart city's energy management system and send only aggregated, encrypted results to central servers. This minimizes the amount of sensitive data that needs to be transmitted over the network, reducing the risk of exposure.

5 | Case Studies: Securing Data Transmission in Artificial Intelligence-Internet of Things Networks

Several real-world applications demonstrate how secure data transmission can be achieved in AI-enabled IoT networks. These case studies highlight different approaches to tackling security challenges in diverse sectors, including smart cities, healthcare, and industrial IoT. The case studies underscore the importance of implementing robust, scalable, and adaptive security mechanisms to ensure the integrity and confidentiality of transmitted data.

5.1 | Smart City: Barcelona's Internet of Things-Based Urban Infrastructure

Background

Barcelona, a leading smart city, has embraced IoT and AI to enhance its urban infrastructure. The city uses an extensive network of IoT sensors and devices to monitor and manage various services, including traffic, waste management, street lighting, and air quality. With over 20,000 IoT devices deployed, securing data transmission in this large-scale network has been a priority to prevent disruptions and unauthorized access to critical infrastructure.

Security challenges

Barcelona's IoT ecosystem is highly heterogeneous, with devices using different communication protocols like Wi-Fi, Zigbee, and LoRaWAN. The diverse nature of these devices introduces vulnerabilities related to data interception, unauthorized access, and potential cyberattacks targeting critical services, such as traffic management systems or smart lighting controls.

Solution

Barcelona has implemented several measures to secure data transmission within its smart city infrastructure:

I. Blockchain-based key management: the city employs blockchain technology to securely manage encryption keys across its IoT network. The decentralized nature of blockchain ensures that no single entity can tamper with or gain control over encryption keys, preventing key compromise in the network.

II. Edge computing: to reduce latency and enhance security, edge computing processes data locally at the edge of the network, such as traffic and environmental sensors. Edge devices encrypt data before transmitting it to central servers, reducing the risk of interception or tampering during transmission.

III. AI-based anomaly detection: AI-powered systems monitor network traffic and detect unusual activity in real-time. If anomalies, such as unexpected data spikes or unauthorized access attempts, are detected, security measures are activated to mitigate potential cyberattacks.

Outcome

Barcelona has successfully secured its IoT-based urban infrastructure by combining blockchain, edge computing, and AI-driven security mechanisms. The city has minimized data breaches, ensured secure communication between devices, and reduced the risk of cyberattacks on critical public services.

5.2 | Healthcare: Securing Data Transmission in Wearable Internet of Things Devices

Background

Wearable IoT devices, such as smartwatches and health monitors, are widely used in healthcare to collect real-time health data from patients. These devices transmit sensitive medical information, including heart rate, glucose levels, and activity data, to healthcare providers for analysis and diagnosis. The transmission of such sensitive data requires stringent security measures to protect patient privacy and prevent unauthorized access to medical records.

Security challenges

Wearable IoT devices face several security challenges, including:

I. Resource constraints: many wearable devices have limited processing power and battery life, making implementing complex encryption algorithms or authentication protocols difficult.

II. Interoperability: wearable devices often need to communicate with various healthcare systems and mobile devices, each with different security standards and protocols. Ensuring consistent security across these platforms is challenging.

III. Data privacy: transmitting sensitive health data over wireless networks increases the risk of data interception, unauthorized access, and patient privacy breaches.

Solution

To address these challenges, healthcare providers and device manufacturers have implemented the following security measures:

I. Lightweight encryption: ECC encrypts data transmitted from wearable devices to healthcare servers. It provides robust encryption with shorter key lengths, making it ideal for resource-constrained devices while ensuring secure data transmission.

II. Secure bluetooth communication: BLE communication between wearables and mobile devices is secured using the DTLS protocol. DTLS encrypts data transmitted over BLE, preventing eavesdropping and tampering.

III. Federated learning for AI models: healthcare providers have started using federated learning, in which AI models analyzing patient data are trained locally on devices without sharing raw data with central servers. This reduces the amount of sensitive data transmitted, protecting patient privacy while improving AI model performance.

Outcome

By employing lightweight encryption, secure communication protocols, and federated learning, wearable IoT devices in healthcare can securely transmit sensitive medical data. These measures have improved patient privacy, minimized the risk of data breaches, and enhanced the trustworthiness of wearable health technologies.

5.3 | Industrial Internet of Things: Securing Data in Siemens' Smart Factories

Background

Siemens [34] has integrated IoT and AI technologies into its smart factories to improve automation, monitoring, and production efficiency. Smart factories use a vast network of IoT sensors to collect real-time data from machinery, production lines, and industrial processes. AI algorithms transmit This data to central systems for analysis and optimization.

Security challenges

Smart factories face numerous security challenges:

I. Real-time data transmission: industrial IoT networks require real-time data transmission with minimal latency to maintain production efficiency. Implementing security measures, such as encryption and authentication, can introduce delays that negatively impact performance.

II. Scalability: large-scale IoT deployments in smart factories involve thousands of devices, making secure key management and software updates difficult to manage.

III. Evolving cyber threats: industrial IoT networks are prime targets for cyberattacks, including ransomware, industrial espionage, and sabotage. Attackers may exploit vulnerabilities in communication protocols or industrial control systems to disrupt operations or steal sensitive data.

Solution

Siemens [34] has adopted several strategies to secure data transmission in its smart factories:

I. Real-time encryption: siemens [34] uses lightweight encryption algorithms like SPECK to secure data transmission between industrial IoT devices and central systems. These algorithms are optimized for real-time communication, ensuring that data remains secure without introducing significant latency.

II. Blockchain for decentralized key management: blockchain technology is used to manage encryption keys decentralized, ensuring secure key exchanges across the network. This approach reduces the risk of key compromise and allows for scalable key management in large IoT deployments.

III. AI-driven security systems: AI-powered IDS monitor real-time network traffic and device behavior. These systems use ML to detect anomalies, such as unauthorized access attempts or unusual data transmission patterns, and trigger automated responses to mitigate threats.

Outcome

Siemens [34] has successfully secured data transmission in its smart factories by using real-time encryption, blockchain-based key management, and AI-driven security solutions. These measures have enhanced the resilience of industrial IoT networks against cyberattacks while ensuring that production efficiency is maintained through secure, low-latency data transmission.

5.4 | Transportation: Securing Autonomous Vehicle Networks

Background

AVs rely on AI and IoT technologies to communicate with surrounding infrastructure, other vehicles, and central systems. These communications involve transmitting real-time data related to traffic conditions, vehicle position, speed, and AI-driven decision-making. Secure data transmission is critical to ensuring the safety and reliability of AV operations.

Security challenges

I. Low-latency requirements: AVs require low-latency communication to make split-second decisions. Implementing security protocols that add latency can compromise the safety and effectiveness of AV systems.

II. MITM attacks: AV networks are vulnerable to MITM attacks, in which an attacker intercepts or alters data between vehicles and infrastructure, potentially causing accidents or traffic disruptions.

III. Data integrity: ensuring data integrity between AVs and infrastructure is critical to preventing false data injection attacks, where an attacker could manipulate data to mislead the vehicle's AI system.

Solution

I. Edge computing and local encryption: AVs use edge computing to process data locally, reducing the need for constant communication with central servers. Local encryption is applied to data before transmitting, ensuring that sensitive information remains protected in transit.

II. Vehicle-to-Everything (V2X) security: secure V2X communication protocols, such as IEEE 1609.2, authenticate and encrypt data exchanges between vehicles and roadside infrastructure. These protocols ensure that only authorized vehicles and devices can participate in the communication network, preventing unauthorized access and data tampering.

III. AI-based threat detection: AI-powered systems continuously monitor data exchanged within the AV network, detecting and mitigating potential cyber threats in real-time. AI models are trained to recognize patterns of normal vehicle behavior and can quickly identify deviations that may indicate an attack.

Outcome

By leveraging edge computing, secure V2X protocols, and AI-driven threat detection, AV networks can ensure low-latency, secure data transmission. These measures enhance the safety and reliability of autonomous driving systems, protecting both the vehicles and the surrounding infrastructure from cyberattacks.

6 | Future Trends and Emerging Technologies

As AI-enabled IoT networks evolve, new technologies and approaches are being developed to address the growing security challenges. This section explores the future directions and emerging technologies that will shape the landscape of secure data transmission in AI-IoT networks, particularly in smart cities, healthcare, industry, and transportation.

6.1 | Quantum Cryptography

Overview

Quantum cryptography represents a significant leap forward in securing data transmission, leveraging the principles of quantum mechanics to provide unprecedented levels of security. The most well-known application is **Quantum Key Distribution (QKD)**, which allows encryption keys to be exchanged securely using quantum particle properties, such as photons.

Key benefits

I. Unbreakable encryption: any attempt to intercept or eavesdrop on quantum-encrypted communication immediately alters the quantum state of the particles, making it detectable. This property ensures that data remains secure from current and future attacks, including those from quantum computers.

II. Future-proofing security: as quantum computing advances, many traditional cryptographic techniques, such as RSA and ECC, will be vulnerable. Quantum cryptography offers a solution that can protect against the decryption power of quantum computers, future-proofing AI-IoT networks.

Challenges

I. Resource-intensive: the current implementations of quantum cryptography require specialized hardware and significant computational resources, which may not be suitable for resource-constrained IoT devices.

II. Scalability: while QKD is promising, its deployment in large-scale AI-IoT networks remains challenging due to the high cost of quantum communication infrastructure and the limited distance over which quantum signals can be transmitted reliably.

6.2 | Post-Quantum Cryptography

Overview

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to be secure against quantum computers. Unlike quantum cryptography, PQC can run on classical computing infrastructure, making it more practical for IoT networks that lack quantum communication capabilities.

Key benefits

I. Compatibility with current systems: PQC algorithms can be integrated into existing AI-IoT networks without requiring specialized hardware, making them easier to adopt on a large scale.

II. Preparedness for quantum threats: by transitioning to PQC, AI-IoT networks can safeguard themselves from future quantum-based attacks, ensuring long-term data security.

Challenges

I. Efficiency: PQC algorithms are often more computationally demanding than current cryptographic techniques, which can be a drawback for IoT devices with limited resources. Researchers are focusing on optimizing these algorithms for low-power and low-memory environments.

II. Standardization: standardizing PQC algorithms is ongoing, and there is no widely accepted set of protocols yet. Organizations must stay agile and adapt to changes as standards are established.

6.3 | Artificial Intelligence-Powered Adaptive Security

Overview

AI-powered security systems that use ML and DL techniques are set to revolutionize how IoT networks defend against cyber threats. These systems continuously learn from network behavior and adapt their defense strategies in real time, improving their ability to detect and respond to new or emerging threats.

Key benefits

I. Anomaly detection: AI can identify unusual patterns in network traffic, device behavior, or user interactions, flagging potential security breaches early. For instance, in a smart city, AI systems could detect abnormal energy consumption in a particular sector and automatically adjust security protocols to prevent an attack.

II. Autonomous response: AI-based systems can go beyond just identifying threats; they can also take corrective action without human intervention. This includes blocking suspicious data transmissions, isolating compromised devices, or updating encryption keys dynamically to maintain secure communications.

III. Continuous learning: AI models continuously improve as they encounter new types of cyberattacks, enabling more effective protection against zero-day vulnerabilities.

Challenges

I. False positives: AI-based systems sometimes generate false positives, flagging benign activities as potential threats. Balancing sensitivity with accuracy remains an ongoing challenge.

II. Data privacy: using AI for security often involves collecting and analyzing large amounts of data from IoT devices, raising privacy concerns. Federated learning is one approach that can help address these concerns by training AI models locally on devices rather than transmitting raw data to central servers.

6.4 | Blockchain for Enhanced Internet of Things Security

Overview

Blockchain technology offers a decentralized approach to securing AI-IoT networks. By distributing and validating encryption keys, transaction records, and device identities across a blockchain ledger, IoT systems can eliminate single points of failure and enhance the integrity of data transmission.

Key benefits

I. Decentralized trust: blockchain eliminates the need for centralized authorities to manage encryption keys, making IoT networks more resilient to attacks and ensuring that no single entity can compromise the entire system.

II. Immutability: the blockchain's immutable ledger ensures that all transactions, device interactions, and data transmissions are permanently recorded, providing a transparent audit trail that can help detect tampering or unauthorized access.

III. Smart contracts for automation: smart contracts can automatically enforce security policies, such as verifying devices' identities before they join the network or ensuring that only authorized devices can communicate with critical infrastructure.

Challenges

I. Scalability and performance: blockchain networks can become slow as the number of transactions increases, which can be a problem for large-scale IoT networks requiring real-time communication.

II. Energy consumption: certain blockchain consensus mechanisms, such as proof of work, are energy-intensive and may not be suitable for IoT networks with constrained power resources.

6.5 | Secure Multi-Party Computation

Overview

Secure Multi-Party Computation (SMPC) is an emerging technology that enables multiple parties to collaboratively compute a function over their inputs while keeping those inputs private. This technique is especially useful for AI-enabled IoT networks that process sensitive data without exposing it to external parties or central authorities.

Key benefits

I. Data privacy: SMPC allows IoT devices to perform joint computations, such as aggregating sensor data or training AI models, without sharing raw data. This preserves privacy and reduces the risk of data breaches.

II. Collaborative AI training: in scenarios where data from multiple sources (e.g., different smart city departments or healthcare providers) must be analyzed together, SMPC ensures that sensitive information remains confidential while enabling AI systems to learn from a broader data set.

Challenges

I. Complexity: SMPC protocols are often computationally intensive, making them challenging to implement on resource-constrained IoT devices.

II. Adoption and awareness: while SMPC has great potential, it is still relatively new and not widely adopted in AI-IoT networks. Increased awareness and further technological developments are needed to drive its adoption.

6.6 | 5G and Beyond: Securing Ultra-Fast Internet of Things Networks

Overview

The deployment of 5G networks and the development of future 6G networks will drastically increase the speed and capacity of IoT communications, enabling massive IoT deployments and Ultra-Reliable Low-Latency Communications (URLLC). However, these advancements also introduce new security challenges, such as securing large-scale device connections and ensuring the integrity of fast, high-volume data transmission.

Key benefits

I. Enhanced encryption standards: 5G networks come with built-in encryption and authentication mechanisms designed to handle the massive number of IoT devices that will be connected to them.

II. Edge security: with 5G, more IoT data will be processed at the network edge, requiring robust security protocols at edge devices to protect data locally before it reaches the core network.

III. Network slicing security: 5G enables network slicing, where different IoT applications (e.g., smart transportation, healthcare) are given virtual networks, each with tailored security policies. This enhances isolating and securing critical infrastructure from less sensitive applications.

Challenges

I. Managing device density: the sheer number of devices connected to 5G and future networks creates challenges in managing secure communications and maintaining consistent security policies across a highly dynamic and distributed network.

II. Sophisticated attack vectors: as 5G opens the door to more complex and integrated IoT applications, attackers will develop more sophisticated methods to exploit vulnerabilities in network infrastructure, requiring ongoing innovation in security technologies.

7 | Conclusion

Securing data transmission in AI-enabled IoT networks is a critical challenge as these networks expand in scope and complexity, particularly in smart cities, healthcare, industrial systems, and autonomous transportation. The convergence of AI and IoT promises immense benefits in automation, efficiency, and data-driven insights. Still, it also brings new risks and vulnerabilities, particularly in safeguarding sensitive data against cyberattacks, unauthorized access, and privacy breaches.

The growing interconnectivity of IoT devices, combined with the intelligence provided by AI, amplifies the scale of potential threats, making it essential to adopt comprehensive and dynamic security measures. Traditional approaches to securing data are no longer sufficient in this context. Advanced encryption techniques, decentralized key management, real-time monitoring powered by AI, and cutting-edge technologies like blockchain and quantum cryptography are becoming indispensable in safeguarding these networks.

Key insights and learnings

I. Complexity and heterogeneity of IoT devices: the vast number and diversity of IoT devices, each with varying security capabilities, create a fragmented security landscape. This complexity is compounded by the different communication protocols and standards these devices rely on, further complicating efforts to maintain secure communication channels.

II. AI as both enabler and threat mitigator: while AI enhances IoT networks by enabling intelligent decision-making and automation, it is also a key tool in strengthening security. AI-driven anomaly detection systems can identify suspicious activities, cyberattacks, and vulnerabilities in real time, providing adaptive responses to emerging threats. However, malicious actors also leverage AI to orchestrate more sophisticated attacks, emphasizing the need for continuous innovation in AI-based security defenses.

III. Importance of edge security: the shift towards edge computing in AI-IoT networks plays a crucial role in reducing latency and ensuring faster data processing, but it also demands secure data handling at the edge. Encryption and decentralized processing at the edge help minimize risks by reducing the data sent over vulnerable networks. Secure edge computing solutions and AI-driven security systems are crucial for maintaining the integrity of real-time data transmission, especially in critical applications like AVs or industrial automation.

IV. Emerging technologies for future-proofing security: PQC, blockchain-based key management, SMPC, and quantum cryptography are emerging technologies that show great promise for addressing current and future security challenges. These technologies offer novel ways to protect data in AI-IoT networks by enhancing encryption standards, ensuring data integrity, and enabling secure, decentralized communication. Quantum cryptography, in particular, holds the potential for unbreakable encryption, while PQC ensures resilience against future threats posed by quantum computing advancements.

V. 5G and beyond: the rollout of 5G networks and the anticipated advent of 6G technologies will further increase the complexity and scale of AI-IoT networks, providing ultra-fast communication speeds and low-latency data transmission. These advancements offer great opportunities but also require robust security measures, such as secure network slicing, which isolates different applications for enhanced protection, and enhanced encryption to manage the large influx of IoT devices. Future network technologies will also demand continuous threat detection and innovation in response mechanisms to maintain a secure ecosystem.

Looking ahead

The future of secure data transmission in AI-IoT networks will rely on a combination of advanced technological solutions and forward-thinking security frameworks. As the volume of data generated and

transmitted by IoT devices grows, ensuring secure, real-time communication will become more challenging. Research in emerging fields such as quantum-safe encryption, federated learning, and Distributed Ledger Technologies (DLT) must be accelerated to develop security protocols that can handle the demands of large-scale AI-IoT deployments.

Moreover, industry, academia, and policymakers collaboration will be critical in standardizing security practices and fostering innovation. Governments will play a key role in establishing regulations that prioritize the security of IoT ecosystems while promoting the adoption of cutting-edge security technologies.

Final thoughts

Securing AI-enabled IoT networks is not merely a technical challenge but a societal imperative. As these networks increasingly permeate every aspect of modern life, from urban infrastructure and healthcare to manufacturing and transportation, their security is directly tied to public safety, privacy, and trust. Organizations must adopt a proactive approach to security, embracing adaptive, scalable, and forward-looking solutions that can withstand the evolving landscape of cyber threats.

In conclusion, the path forward for secure data transmission in AI-IoT networks will be shaped by innovations in encryption, decentralized security, and AI-driven defenses. Integrating emerging technologies such as quantum cryptography and blockchain will play a crucial role in building resilient networks, ensuring that AI-IoT systems remain secure, reliable, and capable of driving the next wave of digital transformation. The future of smart cities, autonomous transportation, intelligent healthcare, and connected industries depends on our ability to safeguard the data that fuels them, making secure AI-IoT networks the cornerstone of a connected, intelligent world.

Funding

The author declare that no external funding or support was received for the research presented in this paper, including administrative, technical, or in-kind contributions.

References

[1] Van Hoang, T. (2024). Impact of integrated artificial intelligence and internet of things technologies on smart city transformation. *Journal of technical education science*, *19*(1 (Spec. Issue)), 64–73. https://doi.org/10.54644/jte.2024.1532

[2] Yao, Y. (2022). A review of the comprehensive application of big data, artificial intelligence, and internet of things technologies in smart cities. *Journal of computational methods in engineering applications*, *2*(1), 1–10. https://doi.org/10.62836/jcmea.v2i1.0004

[3] Aminizadeh, S., Heidari, A., Dehghan, M., Toumaj, S., Rezaei, M., Jafari Navimipour, N., … Unal, M. (2024). Opportunities and challenges of artificial intelligence and distributed systems to improve the quality of healthcare service. *Artificial intelligence in medicine*, *149*, 102779. https://doi.org/10.1016/j.artmed.2024.102779

[4] Shahbazi, Z., Shahbazi, Z., & Nowaczyk, S. (2024). Enhancing air quality forecasting using machine learning techniques. *IEEE access*, *12*, 197290–197299. https://doi.org/10.1109/ACCESS.2024.3516883

[5] Maple, C. (2017). Security and privacy in the internet of things. *Journal of cyber policy*, *2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

[6] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE internet of things journal*, *4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

[7] Escamilla-Ambrosio, P. J., Rodríguez-Mota, A., Aguirre-Anaya, E., Acosta-Bermejo, R., & Salinas-Rosales, M. (2018). Distributing computing in the internet of things: cloud, fog and edge computing overview. In *NEO 2016* (pp. 87–115). Cham: Springer, Cham. https://doi.org/10.1007/978-3-319-64063-1_4

[8] Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A survey on the edge computing for the internet of things. *IEEE access*, *6*, 6900–6919. https://doi.org/10.1109/ACCESS.2017.2778504

[9] Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (E-health) systems. *Journal of medical systems*, *40*(12), 263. https://doi.org/10.1007/s10916-016-0597-z

[10] Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE access*, *9*, 28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867

[11] Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). AI-empowered IoT Security for smart cities. *ACM transactions internet technology*, *21*(4), 1–21. https://doi.org/10.1145/3406115

[12] Ajala, O. A., & Balogun, O. A. (2024). Leveraging AI/ML for anomaly detection, threat prediction, and automated response. *World journal of advanced research and reviews*, *21*(1), 2584–2598. https://doi.org/10.30574/wjarr.2024.21.1.0287

[13] Liao, H. J., Richard Lin, C. H., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of network and computer applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

[14] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Vincent Poor, H. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE communications surveys & tutorials*, *23*(3), 1622–1658. https://doi.org/10.1109/COMST.2021.3075439

[15] Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. *Sensors*, *23*(11), 5206. https://doi.org/10.3390/s23115206

[16] Mamun, M. A. Al, & Yuce, M. R. (2019). Sensors and systems for wearable environmental monitoring toward IoT-enabled applications: A review. *IEEE sensors journal*, *19*(18), 7771–7788. https://doi.org/10.1109/JSEN.2019.2919352

[17] Cominola, A., Giuliani, M., Piga, D., Castelletti, A., & Rizzoli, A. E. (2015). Benefits and challenges of using smart meters for advancing residential water demand modeling and management: A review. *Environmental modelling & software*, *72*, 198–214. https://doi.org/10.1016/j.envsoft.2015.07.012

[18] Jain, N. K., Saini, R. K., & Mittal, P. (2019). A review on traffic monitoring system techniques. *Soft computing: theories and applications* (pp. 569–577). Singapore: Springer, Singapore. https://doi.org/10.1007/978-981-13-0589-4_53

[19] Dias, D., & Paulo Silva Cunha, J. (2018). Wearable health devices—vital sign monitoring, systems and technologies. *Sensors*, *18*(8), 2424. https://doi.org/10.3390/s18082414

[20] Thamarai, M., & Naresh, V. S. (2023). Smart self-power generating garbage management system using deep learning for smart cities. *Microprocessors and microsystems*, *98*, 104816. https://doi.org/10.1016/j.micpro.2023.104816

[21] El Khaled, Z., Mcheick, H., & Petrillo, F. (2019). WiFi coverage range characterization for smart space applications. *2019 IEEE/ACM 1st international workshop on software engineering research & practices for the internet of things (SERP4IoT)* (pp. 61–68). IEEE. https://doi.org/10.1109/SERP4IoT.2019.00018

[22] Adewale, T., & Paul, J. (2024). AI, 5G, and IoT: how these technologies are creating the perfect storm for smart systems. https://www.researchgate.net/publication/385855348

[23] de Carvalho Silva, J., Rodrigues, J. J. P. C., Alberti, A. M., Solic, P., & Aquino, A. L. L. (2017). LoRaWAN — a low power wan protocol for internet of things: a review and opportunities. *2017 2nd international multidisciplinary conference on computer and energy science (SpliTech)* (pp. 1–6). IEEE. https://ieeexplore.ieee.org/abstract/document/8019271/authors#authors

[24] Zhang, T., Lu, J., Hu, F., & Hao, Q. (2014). Bluetooth low energy for wearable sensor-based healthcare systems. 2014 IEEE healthcare innovation conference (HIC) (pp. 251–254). IEEE. https://doi.org/10.1109/HIC.2014.7038922

[25] Lee, J. S., Chuang, C. C., & Shen, C. C. (2009). Applications of short-range wireless technologies to industrial automation: A zigbee approach. *2009 fifth advanced international conference on telecommunications* (pp. 15–20). IEEE. https://doi.org/10.1109/AICT.2009.9

[26] Majumdar, S., Subhani, M. M., Roullier, B., Anjum, A., & Zhu, R. (2021). Congestion prediction for smart sustainable cities using IoT and machine learning approaches. *Sustainable cities and society*, *64*, 102500. https://doi.org/10.1016/j.scs.2020.102500

[27] Salama, R., Mohapatra, H., Tülbentçi, T., & Al-Turjman, F. (2025). Deep learning technology: enabling safe communication via the internet of things. *Frontiers in communications and networks*, *6*, 1416845. https://doi.org/10.3389/frcmn.2025.1416845

[28] Shafik, W. (2024). Deep learning impacts in the field of artificial intelligence. In *deep learning concepts in operations research* (pp. 9–26). Auerbach Publications. https://doi.org/10.1201/9781003433309

[29] Maadi, S., Stein, S., Hong, J., & Murray-Smith, R. (2022). Real-time adaptive traffic signal control in a connected and automated vehicle environment: optimisation of signal planning with reinforcement learning under vehicle speed guidance. *Sensors*, *22*(19), 7501. https://doi.org/10.3390/s22197501

[30] Panda, A. K., Lenka, A. A., Mohapatra, A., Rath, B. K., Parida, A. A., & Mohapatra, H. (2025). Integrating cloud computing for intelligent transportation solutions in smart cities: A short review. In *interdisciplinary approaches to transportation and urban planning* (pp. 121–142). IGI Global. http://doi.org/10.4018/979-8-3693-6695-0.ch005

[31] Rathee, G., Khelifi, A., & Iqbal, R. (2021). Artificial intelligence-(AI-) enabled internet of things (IoT) for secure big data processing in multihoming networks. *Wireless communications and mobile computing*, *2021*(1), 5754322. https://doi.org/10.1155/2021/5754322

[32] Pereira, F., Correia, R., Pinho, P., Lopes, S. I., & Carvalho, N. B. (2020). Challenges in resource-constrained IoT devices: energy and communication as critical success factors for future IoT deployment. *Sensors*, *20*(22), 6420. https://doi.org/10.3390/s20226420

[33] Fera, M. A., & Priya, M. S. (2016). A survey on trusted platform module for data remanence in cloud. Proceedings of the international conference on soft computing systems (pp. 689–695). Springer, New Delhi. https://doi.org/10.1007/978-81-322-2674-1_65

[34] Siemens. (2020). *Totally integrated automation — future inside*. https://new.siemens.com/global/en/products/automation/topic-areas/tia.html