Journal of Infrastructure, Policy and Development 2025, 9(3), 11733.
https://doi.org/10.24294/jipd11733

Article

Enhancing cybersecurity in smart cities: A blockchain-based framework for securing IoT data

Mehdi Houichi[1,*], Faouzi Jaidi[1,2], Adel Bouhoula[3]

[1] University of Carthage, Higher School of Communication of Tunis (Sup'Com), Innov'Com Lab\Digital Security Research Lab, Tunis, 2083, Tunisia.
[2] University of Carthage, National School of Engineers of Carthage, Tunis, 2035, Tunisia.
[3] Department of Next-Generation Computing, College of Graduate Studies, Arabian Gulf University, 26671, Kingdom of Bahrain.
*** Corresponding author:** Mehdi Houichi, Email: mehdi.houichi@supcom.tn

CITATION

Houichi M, Jaidi F, Bouhoula A. (2025). Enhancing cybersecurity in smart cities: A blockchain-based framework for securing IoT data. Journal of Infrastructure, Policy and Development. 9(3): 11733. https://doi.org/10.24294/jipd11733

ARTICLE INFO

Received: 6 May 2025
Revised: 5 July 2025
Accepted: 8 August 2025
Available online: 15 October 2025

Abstract: The rapid expansion of smart cities has led to the widespread deployment of Internet of Things (IoT) devices for real-time data collection and urban optimization. However, these interconnected systems face critical cybersecurity risks, including data tampering, unauthorized access, and privacy breaches. This paper proposes a blockchain-based framework designed to enhance the security, integrity, and resilience of IoT data in smart city environments. Leveraging a private blockchain, the system ensures decentralized, tamper-proof data storage, and transaction verification through digital signatures and a lightweight Proof of Work consensus mechanism. Smart contracts are employed to automate access control and respond to anomalies in real time. A Python-based simulation demonstrates the framework's effectiveness in securing IoT communications. The system supports rapid transaction validation with minimal latency and enables timely detection of anomalous patterns through integrated machine learning. Evaluations show that the framework maintains consistent performance across diverse smart city components such as transportation, healthcare, and building security. These results highlight the potential of the proposed solution to enable secure, scalable, and real-time IoT ecosystems for modern urban infrastructures.

Keywords: smart cities, blockchain, IoT security, cybersecurity, data privacy

1. Introduction

The concept of smart cities has rapidly evolved in recent years, driven by the need for efficient urban management, sustainability, and improved quality of life for citizens (De Guimarães et al., 2020). These cities rely on advanced technologies—including the Internet of Things (IoT), artificial intelligence (AI), big data analytics, and cloud computing—to collect and process real-time data across sectors such as transportation, healthcare, energy, and public safety (Houichi et al., 2022). However, the pervasive use of IoT devices with limited computational capabilities and weak security protocols introduces significant cybersecurity challenges, such as unauthorized access, data tampering, Distributed Denial of Service (DDoS) attacks, and ransomware (Paolone et al., 2022). These threats are magnified by the decentralized and large-scale nature of smart city environments, where thousands of interconnected devices operate without consistent security standards or centralized oversight (Aslan et al., 2023). A single compromised node can have cascading effects, potentially disrupting critical services like traffic control, emergency response, and energy distribution (Hashem et al., 2024). Furthermore, the dynamic context of these environ-

ments complicates efforts to maintain data integrity, confidentiality, and availability (Houichi et al., 2021), especially when sensitive information such as location, health records, and financial data is involved (Houichi et al., 2023). Traditional cybersecurity methods—such as firewalls, encryption, and centralized access controls—are increasingly inadequate for protecting IoT ecosystems. Their reliance on centralized architectures and their computational demands make them ill-suited for IoT environments composed of resource-constrained devices (Shahat Osman & Elragal, 2021; Khan et al., 2022). As a result, there is a growing need for scalable, energy-efficient, and decentralized security frameworks (Khanam et al., 2020; Rahardja et al., 2021).

Blockchain technology has emerged as a promising solution to these challenges. Initially developed for cryptocurrencies, blockchain provides a decentralized and tamper-resistant ledger system. Its core properties—immutability, transparency, distributed consensus, and lack of a central authority—make it well-suited for securing IoT networks in smart cities (Khanam et al., 2020; Xihua & Goyal, 2022). In a blockchain network, each transaction is time-stamped, cryptographically linked, and stored in blocks that cannot be modified without network consensus (Alizadeh et al., 2022). For IoT security, blockchain ensures data integrity through immutable records, enables decentralized trust among network participants, and facilitates authentication via digital signatures. Smart contracts further strengthen system security by automating access control and enforcing predefined rules without human intervention (Aggarwal & Kumar, 2021; Rahman & Saifullah, 2022). Blockchain's transparency and traceability also provide a comprehensive audit trail for detecting anomalies and ensuring accountability (Telo, 2023).

In this paper, we propose a blockchain-based framework tailored to the security needs of IoT systems in smart cities. The framework integrates digital signatures, lightweight consensus mechanisms, and smart contracts to protect IoT data from tampering and unauthorized access. It utilizes a private blockchain network to ensure scalable and decentralized data validation, while enabling real-time monitoring and automated threat responses. The rest of this paper is organized as follows: Section 2 reviews related work on blockchain-based IoT security in smart cities. Section 3 presents the proposed solution and system architecture. Section 4 describes the simulation environment and implementation approach. Section 5 concludes with key findings and future research directions.

2. Related work

The integration of blockchain into IoT systems has emerged as a promising solution to address the growing cybersecurity concerns in smart cities. Numerous studies between 2018 and 2024 have examined how blockchain's core features—decentralization, immutability, transparency, and automated trust—can enhance the security, integrity, and resilience of data generated by IoT devices. One of the earliest notable contributions came from Khan and Salah (2018), who presented a comprehensive review of blockchain-based security solutions for IoT networks. Their study identified key vulnerabilities and proposed lightweight consensus models tailored to IoT's constrained resources, but acknowledged the challenges of scalability and

energy efficiency in practical deployments (Khan & Salah, 2018). Building on this foundation, Khare et al. (2020) introduced the *SmartME* platform, a decentralized framework to eliminate reliance on central authorities. While it improved trust and tamper resistance, the system struggled with performance degradation as the number of devices scaled (Khare et al., 2020). Similarly, Rahman et al. (2018) and Pieroni et al. (2018) applied blockchain to real-time cognitive frameworks and energy management, respectively. These works demonstrated enhanced data integrity and transparent transactions but were limited by network latency and high energy consumption under load (Rahman et al., 2018; Pieroni et al., 2018).

Recent efforts have also focused on domain-specific implementations. Alzahrani et al. (2023) applied blockchain to wastewater monitoring systems, proving its efficacy in securing real-time data. However, like other large-scale systems, it struggled with diverse and high-volume data handling (Alzahrani et al., 2023). In the context of energy grids, Hasan et al. (2022) proposed a consortium blockchain for secure energy trading, which improved data integrity and access control but encountered delays during peak usage. Privacy has also been a central concern. While blockchain's transparency is beneficial for accountability, it may expose sensitive data. Yu et al. (2022) and Mahmood et al. (2023) addressed this issue by proposing privacy-preserving models and advanced encryption techniques. Still, the associated high computational costs raised concerns about their feasibility in resource-constrained environments. Rathore et al. (2019) echoed these limitations in their BlockSecIoTNet architecture, which emphasized confidentiality but required optimization for low-power devices. Broader surveys like those of Xie et al. (2023) and Lunardi et al. (2020) further outlined the challenges of integrating blockchain with legacy systems, highlighting the need for lightweight and interoperable consensus mechanisms. Scekic et al. (2018) and Rahman et al. (2021) also explored blockchain's role in fostering decentralized public services, although practical deployment hurdles such as platform interoperability remained unresolved. To address more recent advances, several studies from 2022 to 2024 have explored security strategies in AI-integrated and federated environments. For example, Ali et al. (2025) presented a comprehensive analysis of cybersecurity solutions tailored for AI-driven IoT-enabled smart cities in advanced communication networks. Their study emphasized the need for dynamic threat modeling and adaptive blockchain integration to support real-time, secure data flow across heterogeneous urban infrastructures (Ali et al., 2025). In the domain of encrypted malware detection, Zhang et al. (2025) introduced HyperEye, a lightweight feature fusion model designed to identify unknown malware traffic using deep learning, achieving low-latency inference suitable for edge and IoT contexts. Additionally, Jianping et al. (2024) proposed a federated learning approach for network attack detection using attention-based graph neural networks. Their framework enables decentralized, privacy-preserving learning across IoT nodes while maintaining high detection accuracy, showing strong promise for scalable smart city deployments (Jianping et al., 2024). These recent works reflect a shift toward integrating AI, deep learning, and federated analytics with blockchain to support both decentralization and intelligent, real-time decision-making in secure IoT ecosystems. **Table 1** summarizes the contributions and limitations of the reviewed works.

Table 1. Summary of related work references.

Authors & year	Focus area	Strengths	Weaknesses
Khan and Salah (2018)	Review of blockchain for IoT security.	Comprehensive analysis, identifies challenges.	Resource limitations in IoT.
Khare et al. (2020)	Trustless smart city system.	Decentralization, reduced central authority reliance.	Scalability issues with transaction volume.
Rahman et al. (2018)	Cognitive framework with IoT and blockchain.	Robust real-time data handling.	Network latency and complexity.
Pieroni et al. (2018)	Smart energy grid with blockchain.	Tamper-proof energy transactions.	High energy usage, limited scale.
Alzahrani et al. (2023)	IoT wastewater management with blockchain.	Efficient data integrity in wastewater systems.	Limited support for large data volumes.
Hasan et al. (2022)	Energy trading in smart grids.	Secure access and transaction control.	Delays during high-volume use.
Yu et al. (2022)	Systematic review of IoT-blockchain security.	Insight into blockchain-IoT security gaps.	Lack of practical implementation.
Mahmood et al. (2023)	Privacy-preserving decentralized model.	Privacy through encryption.	High energy consumption.
Rathore et al. (2019)	BlockSecIoTNet decentralized architecture.	Confidentiality via smart contracts.	Inefficient for low-resource devices.
Xie et al. (2023)	Survey of blockchain in smart cities.	Categorization of research gaps.	No hands-on validation.
Lunardi et al. (2020)	Context-based consensus mechanisms.	Low-latency validation.	High computational demands.
Scekic et al. (2018)	Decentralized smart city governance.	Fosters public trust.	Interoperability challenges.
Rahman et al. (2021)	Real-time data processing with blockchain.	Real-time smart city service support.	Overhead from system complexity.

In summary, the literature demonstrates that blockchain significantly enhances IoT security through decentralized control, data immutability, and automated verification. However, common challenges persist—particularly scalability, energy efficiency, and interoperability with existing infrastructures (Liu et al., 2021). These gaps underline the need for optimized blockchain models tailored to the heterogeneous and large-scale nature of smart cities.

3. Proposed framework

This section presents a comprehensive blockchain-based framework designed to enhance the security, integrity, and efficiency of IoT data in smart city environments. Our proposed solution addresses the primary challenges identified in related works, focusing on scalability, real-time processing, and robust anomaly detection. The solution uses blockchain technology to store, verify, and protect data generated by IoT devices in a decentralized and tamper-proof manner.

3.1. Overview of the proposed framework

The proposed framework leverages blockchain technology to securely manage and verify data generated by IoT devices across a smart city, offering robust protection against cybersecurity threats such as data tampering, unauthorized access, and manipulation of critical functions. By utilizing a decentralized approach, the framework eliminates reliance on a central authority, thereby enhancing system resilience and ensuring data integrity (Houichi et al., 2024). In this setup, IoT devices, including

smart sensors and meters, continuously gather real-time data on various metrics such as traffic flow, energy consumption, and environmental conditions. Each IoT device is assigned a unique digital signature, which acts as a cryptographic identity, ensuring that data transmitted to the blockchain originate from an authenticated and authorized source. This prevents unauthorized devices from compromising the system. The backbone of this solution is a private blockchain network that records every interaction between IoT devices and the system. Each transaction, whether a data submission or a verification, is stored immutably, ensuring the permanence and integrity of all records. The blockchain's decentralized ledger eliminates the risk of single points of failure and prevents retrospective tampering with previously stored data. To maintain data security and authenticity, authorized nodes (validators) play a critical role. These validators use smart contracts to enforce predefined security policies, ensuring that only trusted and valid data is appended to the blockchain. Additionally, the system integrates anomaly detection mechanisms that continuously monitor data flows for abnormal patterns, such as sudden spikes in sensor activity or irregular traffic, flagging potential security threats in real-time. This decentralized verification process ensures that any malicious data or suspicious activity is quickly identified, preventing its inclusion in the blockchain and thereby maintaining a high level of trustworthiness in the smart city's data ecosystem. This integrated framework not only enhances security but also facilitates a highly transparent and accountable environment, crucial for the smooth functioning of various smart city services. Through the use of digital signatures, smart contracts, and anomaly detection, the framework is designed to safeguard the integrity of IoT data and ensure reliable, real-time decision-making across the city's infrastructure. **Figure 1** illustrates the layered design of the system.

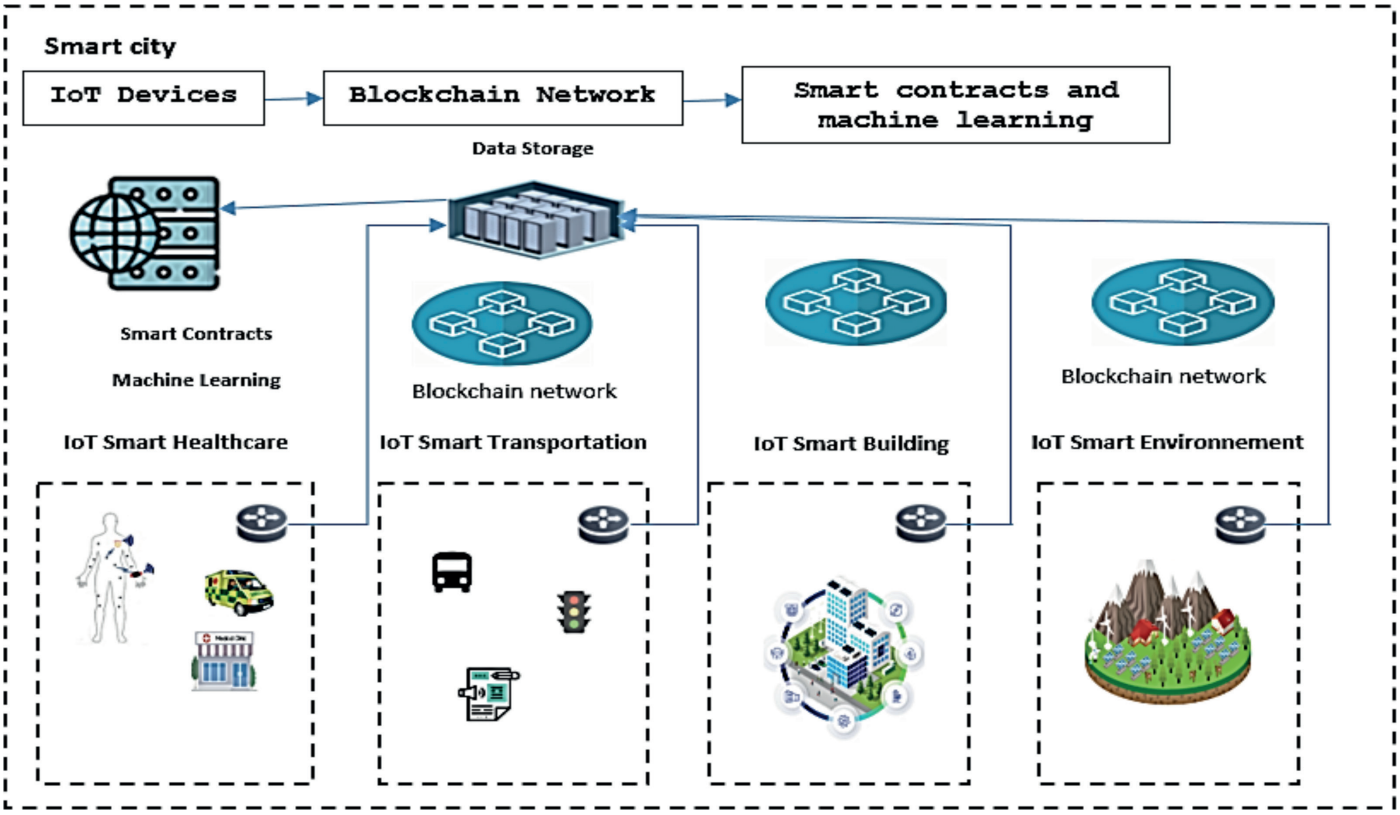

Figure 1. Blockchain-based framework for securing IoT data.

3.2. Description and workflow of the framework

Our system is structured around three core layers—as illustrated in **Figure 1**—each designed to ensure robust security, scalability, and resilience across the smart city infrastructure. These layers are the following: (1) **the data collection layer**, responsible for gathering information from the environment; (2) **the blockchain layer**, which handles data validation and immutable storage; and (3) **the smart contracts and machine learning layer**, which manages automated enforcement and anomaly detection. Each of the six components described below operates within one of these three core layers:

1) **IoT devices and sensors**: These devices are responsible for collecting data across different sectors of the smart city, such as transportation, energy, and environment monitoring. Each device generates data at regular intervals and transmits it to the blockchain. The digital signature assigned to each device ensures that data originates from a trusted source, preventing unauthorized access and data manipulation. IoT devices within the system are lightweight, which is critical for ensuring seamless data collection without overloading the system or compromising energy efficiency.
2) **Private blockchain network**: The blockchain acts as the core data storage and verification system. Transactions from IoT devices (data submissions) are verified using a consensus mechanism of Proof of Work (PoW) to ensure only valid and authentic data is stored. This private blockchain ensures that only authorized nodes can participate in the network, maintaining confidentiality while securing data integrity. Once the data is validated, it is immutably stored in the blockchain, preventing any further modification or tampering.
3) **Validators (authorized nodes)**: Validators play a crucial role in maintaining the integrity of the system. These authorized nodes verify the incoming data by checking the digital signatures associated with each IoT device and confirming the authenticity of the data. They also ensure compliance with pre-defined security policies, identifying any potential anomalies that could indicate data manipulation or cyberattacks. Validators collaborate to maintain decentralized control, and only after successful validation is the data added to the blockchain.
4) **Transaction layer**: The transaction layer manages the transmission of data from IoT devices to the blockchain. Every piece of data submitted by an IoT device is treated as a cryptographically signed transaction. Using its private key, each IoT device encrypts the data before transmission, ensuring that only authorized devices can interact with the system and protecting the data from unauthorized access or tampering during transit. This layer also handles the integrity of the transaction process by timestamping and authenticating each submission.
5) **Consensus layer**: This layer is responsible for validating transactions in the blockchain. Validators use a consensus algorithm to verify the authenticity of the data before it is added to the blockchain. In the proposed framework, PoW is employed as the consensus mechanism. Although PoW is computationally

intensive, it provides a high level of security by requiring miners to solve complex cryptographic puzzles to validate transactions. This mechanism ensures the integrity and immutability of the blockchain data, making it suitable for environments where trust and robustness are critical. Despite its resource demands, PoW can still be integrated into smart city contexts through optimized configurations that balance performance with security.

6) **Storage layer**: Once the data is validated, it is stored immutably in the blockchain. Each data transaction is recorded in a block, ensuring that historical records cannot be altered or deleted. This provides a tamper-proof audit trail of all IoT activity, which is critical for maintaining transparency and accountability in the smart city ecosystem. The immutable storage of data helps prevent malicious actors from altering past transactions, ensuring that all stored data remains trustworthy and reliable for future decision-making processes.

Beyond these layers, the system integrates encryption and anomaly detection mechanisms at every stage of data transmission and validation. Encryption ensures that even if data is intercepted, it cannot be understood or tampered with. Meanwhile, anomaly detection algorithms actively scan for any abnormal patterns in data traffic, such as a sudden spike in data flow from a sensor, which may signal a potential security threat. In such cases, the system can flag the transaction for further analysis before it is added to the blockchain, enhancing the overall security of the system. This multi-layered architecture ensures that the smart city's IoT infrastructure remains secure, scalable, and resilient against cyber threats. Each layer works in tandem to provide comprehensive protection for the vast amounts of data generated within the smart city, ensuring both the confidentiality and integrity of the system while maintaining high levels of performance. **Figure 2** outlines the data flow through these components, from initial collection to storage.

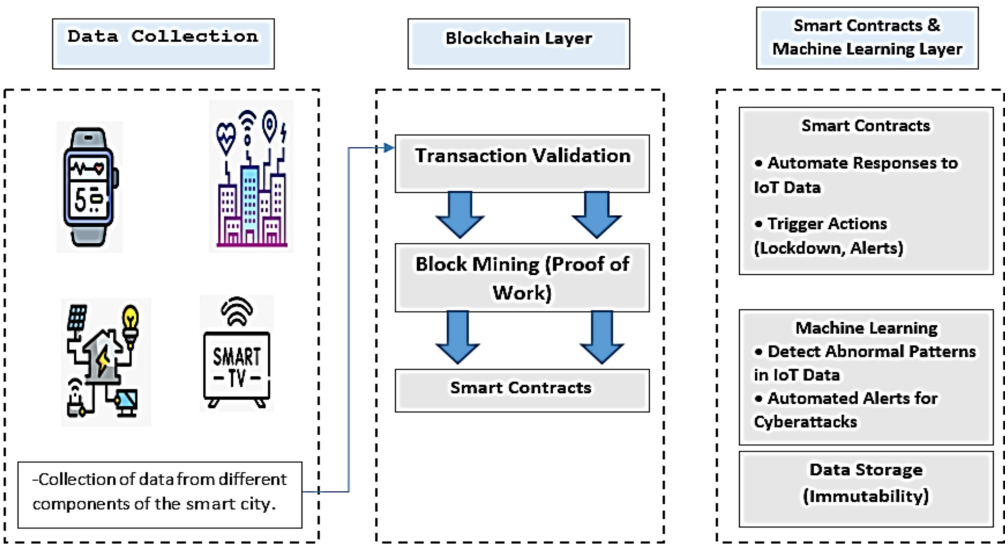

Figure 2. Layers for our approach.

3.3. Use case: smart city traffic monitoring with blockchain and anomaly detection

Let's explore an in-depth use case where smart city traffic monitoring is integrated with our blockchain-based IoT security framework. In this scenario, IoT sensors deployed across key intersections and roadways in the city provide real-time monitoring of traffic conditions, as shown in **Figure 3**. The system ensures secure data transmission, validation, and storage using blockchain technology, and it also incorporates anomaly detection mechanisms to identify potential issues in traffic patterns.

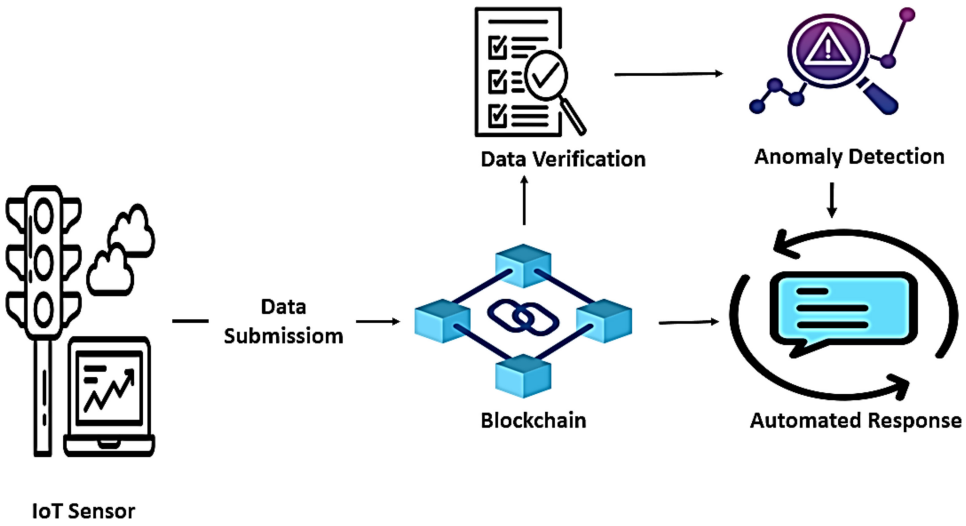

Figure 3. Use case: traffic monitoring in smart cities.

3.3.1. IoT traffic sensors

At the core of this traffic monitoring use case are IoT traffic sensors strategically deployed across the city, particularly at key intersections, highways, and major roadways. These sensors are designed to collect real-time data on traffic conditions, including metrics such as vehicle count, congestion levels, and road conditions. These sensors can track vehicle flow, detect congestion, and monitor environmental factors like road temperature or moisture, ensuring comprehensive traffic management. To ensure the authenticity and security of the data, each sensor is assigned a unique digital signature, which guarantees that any data submitted to the system originates from a trusted source. The use of digital signatures prevents unauthorized devices from feeding false data into the network, maintaining the reliability of the system.

3.3.2. Data submission

Every few minutes, the IoT traffic sensors transmit the collected data to the blockchain network for secure storage and verification. The transmission process is secured using cryptographic techniques, with the data being encrypted and signed by the sensor's private key before submission. This guarantees that the data has not been tampered with during transmission and can only be decrypted by authorized entities within the blockchain network. The digital signature attached to the data serves as proof that the information is coming from a legitimate source, ensuring that no unauthorized data can be introduced into the system. Through this mechanism, the system maintains a high level of security and ensures that all data entering the blockchain are valid and trustworthy.

3.3.3. Data verification

Once the traffic data reaches the blockchain, it is verified by authorized nodes (validators). These validators are responsible for ensuring the integrity of the data by checking the digital signature using the sensor's public key. If the signature matches, the data is deemed valid and is added to the blockchain as a permanent, immutable record. This ensures that each data entry is traceable and cannot be altered once it is added, providing a secure audit trail of traffic conditions across the city. In cases where the digital signature is invalid, the transaction is rejected, preventing unauthorized or corrupted data from entering the blockchain. This layer of data verification is critical for ensuring that the traffic data stored in the blockchain is accurate and tamper-proof.

3.3.4. Anomaly detection

The **anomaly detection system** is an integral part of the traffic monitoring framework, continuously analyzing incoming data to identify any irregular patterns or suspicious activities. Using machine learning models and predefined thresholds, the system can detect anomalies such as sudden spikes in vehicle count, unusual congestion patterns, or erratic sensor behavior. For instance, if there is an unexpected increase in traffic at an intersection, which deviates from the typical pattern for that time of day, the system flags the data for further review. The anomaly detection system acts as an early warning mechanism, preventing potentially compromised data from being stored in the blockchain. By detecting and flagging irregularities in real-time, the system enhances the security and accuracy of traffic data, ensuring that only valid and expected data is recorded.

3.3.5. Automated response with smart contracts

Smart contracts form a crucial component of the system's automated response mechanism. These are self-executing contracts programmed to carry out specific actions when certain conditions are met. In the context of traffic monitoring, smart contracts can be triggered to perform a variety of actions based on real-time data from IoT sensors. For example, if the system detects severe traffic congestion at an intersection, the smart contract could automatically adjust the timing of traffic lights to alleviate the congestion. Alternatively, if a traffic incident is detected, the system could notify city authorities to deploy additional resources such as traffic management teams or emergency services. These automated responses allow the system to react instantly to changing traffic conditions without the need for manual intervention, improving the efficiency of traffic management and ensuring that problems are addressed promptly. This capability helps maintain smooth traffic flow and optimizes the use of city resources, reducing the negative impact of congestion on urban mobility.

The integration of blockchain with IoT-based traffic monitoring offers several critical benefits to smart city infrastructure (Houichi et al., 2024). First, the system enhances security by ensuring that all traffic data is encrypted, authenticated, and stored immutably in the blockchain. Unauthorized data cannot enter the system, and any anomalies are detected in real-time. Second, the system provides data integrity and transparency, with each transaction being traceable and tamper-proof. This creates a clear audit trail, valuable for long-term urban planning and accountability.

Third, the use of smart contracts and automated anomaly detection makes the system scalable and efficient, minimizing the need for human oversight and enabling real-time decision-making. Lastly, the system's ability to monitor traffic in real-time allows for immediate responses to traffic incidents, helping city planners manage congestion and optimize urban mobility more effectively. Through these capabilities, the system delivers a robust and scalable solution for improving the management of traffic in smart cities.

3.4. Discussion

The proposed blockchain-based framework provides a robust solution to enhance the security, integrity, and scalability of IoT data in smart city environments. By leveraging digital signatures, decentralized validation, and anomaly detection mechanisms, the system effectively addresses cybersecurity threats such as unauthorized access, data tampering, and system manipulation. The integration of smart contracts further strengthens the system's ability to automate responses in real time, ensuring rapid reaction to potential anomalies. This decentralized approach eliminates reliance on a central authority, improving system resilience and transparency. While the framework offers significant advantages, including energy-efficient consensus mechanisms and scalable architecture, future research should focus on refining machine learning models for anomaly detection and exploring more decentralized consensus algorithms. The next section delves into the specific use case implementation and further evaluates the system's performance in a real-world smart city context.

4. Simulation and evaluation

The successful simulation of a blockchain-based security framework for IoT devices in a smart city requires careful selection of tools and technologies that can support decentralized architectures and real-time processing. For this purpose, Python was selected as the primary programming language, due to its versatility, wide adoption, and the extensive range of libraries available for blockchain development, cryptographic operations, and network simulation.

4.1. Environment and tools

This section outlines the key tools and libraries used to build and simulate the smart city security framework. The core of the simulation revolves around mimicking a real-world smart city IoT environment, where numerous devices communicate securely through a decentralized blockchain network. Each component of the framework was selected to ensure scalability, flexibility, and security during both normal operations and potential cyberattacks.

Flask: Flask is a lightweight web framework that was employed to build a user interface (UI) for managing and monitoring blockchain activity (Sirena & Patti, 2022). Flask's simplicity and modular design made it ideal for real-time visualization and interaction with the system. Through the UI, users can interact with the blockchain by submitting transactions, reviewing the chain, and monitoring IoT device activity. The web interface acts as a central control point, allowing stakeholders to view and analyze data flows, validate blockchain transactions, and assess the status of IoT

devices in the simulated smart city. Flask also supports RESTful API creation, which can be used to integrate various IoT device simulations into the blockchain network.

Pycryptodome: To secure communication between IoT devices and the blockchain, Pycryptodome, a powerful Python cryptography library, was used. This library provides all the cryptographic functions needed to establish secure connections (Majeed et al., 2021), including:

Key generation: As part of the decentralized framework, each IoT device generates its own public–private key pair, which is used to encrypt data sent to the blockchain. Pycryptodome's RSA module was used to generate asymmetric keys for secure communication (Morchid et al., 2024).

Encryption/Decryption: Data from IoT devices, such as sensor readings, are encrypted using the device's private key before being sent to the blockchain. The blockchain nodes can decrypt the data using the corresponding public key to verify the authenticity of the sender.

Digital signatures: Pycryptodome's signature module was employed to generate digital signatures for each transaction initiated by an IoT device. These signatures ensure that the data has not been tampered with during transmission, and the recipient (blockchain node) can verify the origin of the data (Baucas & Spachos, 2021).

Data verification: Upon receiving data from an IoT device, blockchain nodes use the public key of the sending device to verify the authenticity of the signature. This prevents unauthorized or malicious actors from introducing false data into the blockchain, ensuring data integrity throughout the network.

4.2. Algorithm for our approach

In the proposed Blockchain-Based IoT Security for Smart Cities system, the algorithm (referred to as Algorithm 1: Blockchain-Based IoT Security for Smart Cities) is designed to secure data communication among IoT devices in smart city environments using blockchain technology. The algorithm begins by collecting data from various IoT devices across multiple smart city components such as traffic sensors, security cameras, and health monitors. These devices continuously generate data, which is then encrypted and signed using public–private key pairs to ensure secure transmission. Once the data is encrypted and signed, it is submitted to the blockchain network in the form of transactions, as described in Step 3. These transactions are validated by verifying the digital signatures using the public keys of the respective IoT devices. If a transaction is deemed valid, it is included in a block that is mined using a PoW consensus mechanism, ensuring that the new block is securely added to the blockchain ledger (Step 4). The blockchain is monitored in real-time to track the data submitted by various IoT devices. This is accomplished via a web-based dashboard that displays the relevant data from the blockchain, allowing stakeholders to visualize the status of the smart city components (Step 5 and Step 6). The algorithm also includes a security enhancement phase where anomaly detection algorithms are employed to monitor for abnormal patterns, such as traffic anomalies or potential security breaches (Step 7). In the event of a detected anomaly, the compromised IoT device or network node is isolated, and the system administrator is notified. The system responds to security breaches through automated isolation processes facilitated

by smart contracts, and the blockchain ledger is updated after each block is mined, ensuring the integrity and transparency of the data (Step 8 and Step 9). This approach provides a robust and decentralized solution for securing IoT data in smart city ecosystems, enhancing both security and real-time monitoring capabilities.

Algorithm 1: Blockchain-Based IoT Security for Smart Cities

Inputs:

- IoTData: Data from IoT devices (e.g., traffic sensors, security cameras, health monitors)
- PublicPrivateKeys: Public-private key pairs for IoT devices

Outputs:

- TransactionBlock: A new block added to the blockchain
- Blockchain: Updated blockchain ledger

```
Procedure SecureIoTData(IoTData, PublicPrivateKeys)
// Step 1: IoT Device Data Collection
for each device in IoTDevices do
    deviceData ← CollectData(device)
    IoTData.append(deviceData)
end for

// Step 2: Data Encryption and Signature Generation
for each data in IoTData do
    privateKey ← PublicPrivateKeys[data.deviceID].private
    signedData ← Sign(data, privateKey)
    encryptedData ← Encrypt(data, privateKey)
    Transactions.append({signedData, encryptedData, deviceID})
end for

// Step 3: Transaction Creation and Submission
for each tx in Transactions do
    SubmitTransaction(tx)
end for

// Step 4: Block Mining and Validation
if Transactions.count ≥ threshold then
    block ← []
    for each tx in Transactions do
        isValid ← Verify(tx, PublicPrivateKeys[tx.deviceID].public)
        if isValid then
            block.append(tx)
        else
            RejectTransaction(tx)
        end if
    end for
    newBlock ← MineBlock(block)
    Blockchain.append(newBlock)
end if
```

```
// Step 5: Real-Time Monitoring
for each tx in Blockchain.latestBlock do
    DisplayOnDashboard(tx)
end for

// Step 6: Smart City Visualization
for each component in SmartCityComponents do
    VisualizeData(component)
    if AnomalyDetected(component) then
        Highlight(component)
    end if
end for

// Step 7: Anomaly Detection
for each block in Blockchain do
    RunAnomalyDetection(block)
    if AnomalyFound then
        TriggerAlert()
    end if
end for

// Step 8: Response to Security Breaches
if BreachDetected then
    IsolateCompromisedDevice()
    NotifyAdmin(deviceID, timestamp)
    DeploySmartContractResponse()
end if

// Step 9: Ledger Update
UpdateBlockchainLedger()
End Procedure
```

4.3. Simulation

4.3.1. Simulation of blockchain for securing smart city

The first phase of the simulation focuses on implementing a blockchain system to secure various IoT devices in a smart city environment. The components simulated include smart buildings, smart healthcare, and smart transportation, with devices like security cameras, smart meters, health monitors, and traffic sensors connected to a central blockchain-based server for each domain. Each IoT device in the smart city has been equipped with a unique public–private key pair, generated using RSA cryptography. These devices securely communicate with the blockchain network by signing the data they generate (e.g., traffic counts, health readings, security alerts) with their private keys. The blockchain system, which we implemented using Python and Flask, acts as the backbone of this decentralized system, where data is validated, stored, and monitored. For example, in the smart transportation system, traffic sensors generate data about vehicle counts on roads. This data is signed with the device's private key and submitted to the blockchain network via a RESTful API. Once submitted, the data is validated using the traffic sensor's public key, and if valid, it is

```python
from Crypto.Signature import pkcs1_15
from Crypto.Hash import SHA256
from Crypto.PublicKey import RSA
import requests

# Load private key for the traffic sensor
with open('traffic_sensor_private.pem', 'rb') as f:
    private_key = RSA.import_key(f.read())

# Sign the data
def sign_transaction(transaction_data):
    h = SHA256.new(transaction_data.encode('utf-8'))
    signature = pkcs1_15.new(private_key).sign(h)
    return signature.hex()

# Data transmission
transaction_data = "Traffic_Sensor_1-Central_Server-Vehicle_Count: 150"
signature = sign_transaction(transaction_data)

# Send data to the blockchain server
transaction = {
    'sender': 'Traffic_Sensor_1',
    'recipient': 'Central_Server',
    'data': transaction_data,
    'signature': signature
}
response = requests.post('http://127.0.0.1:5000/transactions/new', json=transaction)
print("Transaction Response:", response.status_code)
```

Figure 4. Blockchain and mining process.

added to the next block. Each block is mined using the PoW consensus mechanism before being appended to the blockchain. **Figure 4** is an example of how traffic sensors communicate with the blockchain using digital signatures and encryption:

The blockchain network receives transactions from IoT devices and adds them to a block after validation. The PoW mechanism ensures that the data is securely added to the blockchain, preventing malicious attacks as shown in **Figure 5**.

```python
# Blockchain block creation
def mine():
    last_block = blockchain.last_block
    proof = blockchain.proof_of_work(last_block['proof'])

    blockchain.new_transaction(sender="0", recipient="Miner_Address", data="Mining Reward"

    previous_hash = blockchain.hash(last_block)
    block = blockchain.new_block(proof, previous_hash)
    return block
```

Figure 5. Blockchain block creation.

To monitor and manage the blockchain, a web-based dashboard was built using Flask, as shown in **Figure 6**. Through this interface, users can view all blocks in the chain, inspect transactions, and monitor real-time data flow from IoT devices. This user interface is essential for stakeholders to manage the smart city's security infrastructure.

4.3.2. Simulation with smart contracts

In this phase, we extended the blockchain framework by integrating smart contracts to automate actions based on data from IoT devices. Smart contracts are

Blockchain Data

Index	Timestamp	Transactions	Proof	Previous Hash
1	1727507494.3884063		100	1
2	1727507612.741185	• Sender: Building_Security_Camera_1, Recipient: Central_Server, Data: Building_Security_Camera_1-Central_Server-Activity: Normal • Sender: Health_Monitoring_Device_1, Recipient: Hospital_Server, Data: Health_Monitoring_Device_1-Hospital_Server-Heart_Rate: 75 • Sender: Waste_Bin_1, Recipient: Central_Server, Data: Waste_Bin_1-Central_Server-Fill_Level: 75% • Sender: 0, Recipient: 303ca15142dd4a4c888bea55a29fd503, Data: Mining Reward	35293	88f319262153747a2e9f23b5f0ad33336f104d53f775fd3c1ca7f452a6ac4fea

Figure 6. Web interface for blockchain management.

self-executing programs that trigger predefined actions when specific conditions are met. For example, if a security camera detects suspicious activity, a smart contract is triggered to automatically lock down the building or alert authorities. When the security camera detects suspicious activity, it generates a transaction that is submitted to the blockchain. The smart contract evaluates the transaction, and if the activity is deemed suspicious, it triggers an automated response to lock down the building as shown in **Figure 7**.

The security camera sends data to the blockchain, as shown **Figure 8**, where the smart contract evaluates it:

When suspicious activity is detected, the smart contract triggers the building lockdown as described in **Figure 9**.

```
def smart_contract_action(activity_data):
    if "Suspicious Activity" in activity_data:
        print("Trigger Alert: Building is locked down.")
        # Automated action: lockdown the building
        # This would integrate with a real-world system to control physical access
```

Figure 7. Example of a security camera detecting suspicious activity.

```
transaction_data = "Building_Security_Camera_1-Central_Server-Activity: Suspicious Activit
signature = sign_transaction(transaction_data)
transaction = {
    'sender': 'Building_Security_Camera_1',
    'recipient': 'Central_Server',
    'data': transaction_data,
    'signature': signature
}
response = requests.post('http://127.0.0.1:5000/transactions/new', json=transaction)
```

Figure 8. Example of sending malicious data camera.

```
if "Suspicious Activity" in transaction_data:
    smart_contract_action(transaction_data)
```

Figure 9. Smart contract action.

4.3.3. Simulation with integration of machine learning

In this final phase, we incorporated machine learning models to detect anomalies in the data generated by IoT devices. By integrating machine learning, the system can automatically flag unusual patterns, such as abnormal traffic counts or security breaches. We trained a machine learning model to classify normal versus abnormal data patterns, as shown in **Figure 10**. When IoT devices submit data, the blockchain system uses this model to analyze incoming data in real-time. If an anomaly is detected, an alert is triggered. The workflow involves real-time monitoring of IoT devices, where each incoming transaction is analyzed by the machine learning model. If an anomaly is detected, the system automatically alerts the administrator and may even trigger a smart contract to take corrective action.

```
# Predict if the incoming data is an anomaly
from sklearn.externals import joblib
model = joblib.load('anomaly_detection_model.pkl')

def is_anomaly(data):
    prediction = model.predict([data])
    return prediction == 1  # 1 indicates anomaly

# Check for anomalies in real-time
incoming_data = [150, 75, 30]  # Example IoT data
if is_anomaly(incoming_data):
    print("Anomaly detected!")
```

Figure 10. Real-time anomaly detection workflow.

4.3.4. Evaluation and discussion

The simulation results validate the effectiveness of our blockchain-based IoT security framework in addressing key challenges of data integrity, real-time monitoring, and automated threat response in smart cities. The framework reliably handled secure communication among various IoT devices—including traffic sensors, health monitors, and security cameras—across domains such as transportation, healthcare, and smart buildings. It achieved fast transaction validation and efficient block creation, ensuring minimal delay in processing critical urban data. The integration of machine learning enhanced the system's capability to detect anomalies, such as abnormal traffic patterns or unauthorized data submissions, allowing for proactive mitigation. Furthermore, the use of smart contracts enabled automated enforcement of security policies, such as isolating compromised devices or notifying administrators without manual intervention. The system maintained consistent performance during diverse simulations, demonstrating both scalability and adaptability to the dynamic requirements of modern smart cities. Overall, the framework offers a resilient and decentralized approach to securing urban infrastructures through real-time data protection, anomaly detection, and automated response mechanisms.

Although the current simulation demonstrates the core components of the framework using synthetic IoT data, its architecture is designed with scalability and interoperability in mind. The modular nature of the private blockchain setup allows for seamless registration of new IoT devices and smart contracts without reconfiguring the network. This enables horizontal scalability to accommodate large-scale deployments across smart city applications. In terms of interoperability, the framework relies on standardized interfaces (RESTful APIs, JSON structures) and communication protocols (such as HTTP/S and MQTT). These features allow integration with existing IoT middleware and legacy smart city systems, facilitating adoption in diverse operational environments. Future deployments can incorporate off-chain data handling mechanisms like IPFS to enhance performance under heavy data loads.

5. Conclusion and future work

Our proposed blockchain-based security framework for smart cities represents a comprehensive solution for securing IoT data across various components, including smart transportation, healthcare, and building management. By leveraging blockchain's decentralized nature and integrating cryptographic methods, our framework ensures data integrity, transparency, and resilience against cyberattacks. The system efficiently handles real-time data processing from IoT devices and enables secure transactions through digital signatures and encryption, validated by blockchain's immutability. Throughout the simulation, the framework demonstrated high performance in transaction validation, block mining, and automated responses to anomalies. The use of smart contracts further enhanced security by automating predefined actions when anomalies or threats were detected. Additionally, the integration of machine learning models successfully flagged abnormal data patterns, providing an additional layer of protection and enabling proactive responses to potential cyber threats. The results of our simulation show that the framework is robust, scalable, and effective in safeguarding IoT data in a smart city environment. Our solution enhances the real-time decision-making processes of city administrators, ensuring the secure and smooth operation of urban services. The framework's adaptability across multiple smart city components, from traffic management to healthcare systems, makes it a versatile approach to smart city security.

Although the current implementation has proven successful, future work will focus on expanding and improving the system in several key areas:

Exploring different machine learning models: We plan to evaluate the performance of more advanced machine learning and deep learning methods, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). These models will offer enhanced anomaly detection and system intelligence, allowing for more sophisticated and robust identification of abnormal patterns in IoT data.

Testing with larger datasets: Our future evaluations will include larger-scale simulations with thousands of IoT devices from various smart city sectors. This will test the framework's ability to scale while maintaining performance, ensuring the system can handle the increased data flow typical of larger urban environments.

Integration of additional IoT components: We plan to extend the framework to include more smart city components such as smart energy management, waste

management, and public safety systems. This will provide a more comprehensive assessment of the system's adaptability and efficiency in managing data from a wider range of sources, ensuring that the model can handle diverse urban services.

Enhanced consensus mechanisms: We aim to explore more energy-efficient and scalable consensus mechanisms, such as Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT). These mechanisms will optimize the system's scalability and reduce the computational burden associated with traditional PoW consensus models, especially in resource-constrained environments.

Real-world testing and deployment: In addition to simulations, future work will focus on deploying the framework in real-world smart city environments to test its performance under actual operating conditions.

This will involve collaboration with city planners and IoT infrastructure providers to assess how well the system integrates with existing smart city systems.

By focusing on these areas, we expect to further enhance the security, scalability, and performance of our framework, making it even more robust and adaptable to the evolving needs of modern smart cities. With continued optimization, our blockchain-based IoT security framework will provide a reliable foundation for the secure, real-time operation of smart city infrastructures.

Author Contributions: Conceptualization, MH and FJ; methodology, MH; software, MH; validation, MH, FJ and AB; formal analysis, MH; investigation, MH; resources, FJ; data curation, MH; writing—original draft preparation, MH; writing—review and editing, FJ and AB; visualization, MH; supervision, FJ and AB; project administration, FJ. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank Innov'Com Lab (Sup'Com) for providing administrative and technical support throughout the research.

Conflicts of Interest: The authors declare no conflict of interest.

References

Aggarwal, S., & Kumar, N. (2021). Basics of blockchain. In: Advances in Computers. Elsevier. Volume 121. pp. 129–146. https://doi.org/10.1016/bs.adcom.2020.08.007

Ali, J., Singh, S. K., Jiang W., et al. (2025). A deep dive into cybersecurity solutions for AI-Driven Iot-Enabled smart cities in Advanced Communication Networks. Computer Communications, 229, 108000. https://doi.org/10.1016/j.comcom.2024.108000

Alizadeh, M., Andersson, K., & Schelén, O. (2022). Comparative analysis of decentralized identity approaches. IEEE Access, 10, 92273–92283. https://doi.org/10.1109/ACCESS.2022.3202553

Alzahrani, A. I., Chauhdary, S. H., & Alshdadi, A. A. (2023). Internet of Things (IoT)-Based wastewater management in Smart Cities. Electronics, 12(12), 2590. https://doi.org/10.3390/electronics12122590

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., et al. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Baucas, M. J., & Spachos, P. (2021). Permissioned blockchain reinforced API platform for data management in IoT-based sensor networks. In: 2021 IEEE Global Communications Conference (GLOBECOM). IEEE. pp. 1–6. https://doi.org/10.1109/GLOBECOM46510.2021.9685837

De Guimarães, J. C. F., Severo, E. A., Júnior, L. A. F., et al. (2020). Governance and quality of life in smart cities: Towards sustainable development goals. Journal of Cleaner Production, 253, 119926. https://doi.org/10.1016/j.jclepro.2020.119926

Hasan, M. K., Alkhalifah, A., Islam, S., et al. (2022). Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations. Wireless Communications and Mobile Computing 2022, 9065768. https://doi.org/10.1155/2022/9065768

Hashem, I. A., Siddiqa, A., Alaba, F. A., et al. (2024). Distributed intelligence for IoT-Based smart cities: A survey. Neural Computing and Applications, 1–36. https://doi.org/10.1007/s00521-024-10136-y

Houichi, M., Jaidi, F., & Bouhoula, A. (2021). A systematic approach for IoT cyber-attacks detection in smart cities using machine learning techniques. In: International Conference on Advanced Information Networking and Applications. Springer. pp. 215–228. https://doi.org/10.1007/978-3-030-75075-6_17

Houichi, M., Jaidi, F., & Bouhoula, A. (2022). Analysis of smart cities security: Challenges and advancements. In: 2022 15th International Conference on Security of Information and Networks (SIN). IEEE. pp. 1–5. https://doi.org/10.1109/SIN56466.2022.9970494

Houichi, M., Jaidi, F., & Bouhoula, A. (2023). A comprehensive study of intrusion detection within Internet of Things-based smart cities: Synthesis, analysis and a novel approach. In: 2023 International Wireless Communications and Mobile Computing (IWCMC). IEEE. pp. 505–511. https://doi.org/10.1109/IWCMC58020.2023.10182948

Houichi, M., Jaidi, F., & Bouhoula, A. (2024). Cyber security within smart cities: A comprehensive study and a novel intrusion detection-based approach. Computers, Materials and Continua, 81(1), 393–441. https://doi.org/10.32604/cmc.2024.054007

Jianping, W., Guangqiu, Q., Chunming, W., et al. (2024). Federated learning for network attack detection using Attention-Based graph neural networks. Scientific Reports, 14(1), 19088. https://doi.org/10.1038/s41598-024-70032-2

Kahan, J. H., Allen, A. C., & George, J. K. (2009). An operational framework for resilience. Journal of Homeland Security and Emergency Management, 6(1), 83. https://doi.org/10.2202/1547-7355.1675

Khare, A., Merlino, G., Longo, F., et al. (2020). Design of a trustless smart city system: The #SmartME experiment. Internet of Things, 10, 100126. https://doi.org/10.1016/j.iot.2019.100126

Khan, A. A., Laghari, A. A., Shaikh, Z. A., et al. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-Art review. IEEE Access, 10, 122679–122695. https://doi.org/10.1109/ACCESS.2022.3223370

Khan, M. A., & Salah, K. (2018). IoT Security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khanam, S., Ahmedy, I. B., Idris, M. Y. I., et al. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things. IEEE Access, 8, 219709–219743. https://doi.org/10.1109/ACCESS.2020.3037359

Liu, Y., Qian, K., Wang, K., et al. (2021). Effective scaling of blockchain beyond consensus innovations and Moore's Law: Challenges and opportunities. IEEE Systems Journal, 16(1), 1424–1435. https://doi.org/10.1109/JSYST.2021.3087798

Lunardi, R. C., Alharby, M., Nunes, H. C., et al. (2020). Context-based consensus for appendable-block blockchains. In: 2020 IEEE International Conference on Blockchain (Blockchain). IEEE. pp. 401–408. https://doi.org/10.1109/Blockchain50366.2020.00058

Mahmood, A., Khan, A., Anjum, A., et al. (2023). An efficient and Privacy-Preserving Blockchain-Based secure data aggregation in smart grids. Sustainable Energy Technologies and Assessments, 60, 103414. https://doi.org/10.1016/j.seta.2023.103414

Majeed, U., Khan, L. U., Yaqoob, I., et al. (2021). Blockchain for IoT-Based smart cities: Recent advances, requirements, and future challenges. Journal of Network and Computer Applications, 181, 103007. https://doi.org/10.1016/j.jnca.2021.103007

Morchid, A., Jebabra, R., Ismail, A., et al. (2024). IoT-Enabled fire detection for sustainable agriculture: A Real-Time system using flask and embedded technologies. Results in Engineering, 23, 102705. https://doi.org/10.1016/j.rineng.2024.102705

Paolone, G., Iachetti, D., Paesani, R., et al (2022). A holistic overview of the Internet of Things Ecosystem. IoT, 3(4), 398–434. https://doi.org/10.3390/iot3040022

Pieroni, A., Scarpato, N., Di Nunzio, L., et al. (2018). Smarter city: Smart energy grid based on blockchain technology. International Journal of Advanced Science, Engineering and Information Technology, 8(1), 298–306. https://doi.org/10.18517/ijaseit.8.1.4954

Rahardja, U., Hidayanto, A. N., Lutfiani, N., et al. (2021). Immutability of distributed hash model on blockchain node storage. Scientific Journal of Informatics, 8(1), 137–143. https://doi.org/10.15294/sji.v8i1.29444

Rahman, M., & Saifullah, A. (2022). Transparent and Tamper-Proof event ordering in the Internet of Things platforms. IEEE Internet of Things Journal, 10(6), 5335–5348. https://doi.org/10.1109/JIOT.2022.3222450

Rahman, M. A., Rashid, M. M., Hossain, M. S., et al. (2021). Blockchain and IoT-Based cognitive edge framework for sharing economy services in a smart city. IEEE Access, 7, 18611–18621. https://doi.org/10.1109/ACCESS.2019.2896065

Rahman, M. A., Hossain, M. S., Loukas, G., et al. (2018). Blockchain-Based mobile edge computing framework for secure therapy Applications. IEEE Access, 6, 72469–72478. https://doi.org/10.1109/ACCESS.2018.2881246

Rathore, S., Pan, Y., & Park, J. H. (2019). BlockDeepNet: A blockchain-Based secure deep learning for IoT network. Sustainability, 11(14), 3974. https://doi.org/10.3390/su11143974

Scekic, O., Nastic, S., & Dustdar, S. (2018). Blockchain-Supported smart city platform for social value Co-Creation and exchange. IEEE Internet Computing, 23(1), 19–28. https://doi.org/10.1109/MIC.2018.2881518

Shahat Osman, A. M., & Elragal, A. (2021). Smart cities and big data analytics: A data-driven decision-making use case. Smart Cities, 4(1), 286–313. https://doi.org/10.3390/smartcities4010018

Sirena, P., & Patti, F. P. (2022). Smart contracts and automation of private relationships. In: Constitutional challenges in the algorithmic society. Cambridge University Press. pp. 315–330. https://doi.org/10.1017/9781108914857.017

Telo, J. (2023). Smart city security threats and countermeasures in the context of emerging technologies. International Journal of Intelligent Automation and Computing, 6(1), 31–45.

Xie, J., Tang, H., Huang, T., et al. (2019). A Survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials, 21(3), 2794–2830. https://doi.org/10.1109/COMST.2019.2899617

Xihua, Z., & Goyal, S. (2022). Security and privacy challenges using IoT-Blockchain technology in a smart city: Critical analysis. International Journal of Electrical & Electronics Research, 10(2), 190–195. https://doi.org/10.37391/ijeer.100224

Yu, Z., Song, L., Jiang, L., et al. (2022). Systematic literature review on the security challenges of blockchain in IoT-Based smart cities. Kybernetes, 51(1), 323–347. https://doi.org/10.1108/K-07-2020-0449

Zang, X., Zheng, Z., Zheng, H., et al. (2025). HyperEye: A lightweight features fusion model for unknown encrypted malware traffic detection. IEEE Transactions on Consumer Electronics, 71(2), 5079–5089. https://doi.org/10.1109/TCE.2025.3558353