Evaluating Security Standards and Frameworks for IoT-Enabled Smart Environments

Matthew Lungu
School of Graduate Studies
Copperbelt University
mathewslulu3@gmail.com

Jameson Mbale
School of Information Communications Technology, Copperbelt University.
jameson.mbale@gmail.com

Abstract— The rapid expansion of IoT-enabled smart environments, such as smart homes and cities, brings notable benefits in efficiency, convenience, and sustainability. However, these advancements also introduce significant security risks as the growing interconnectivity of IoT devices increases their vulnerability to threats like data breaches, device hijacking, and DDoS attacks. Ensuring the security of these environments is crucial to mitigate risks and implement effective controls. Despite the urgent need for comprehensive security frameworks, a significant gap remains in identifying standards and methodologies that address the unique and evolving security challenges of IoT-based systems. This paper aims to address this gap by conducting an extensive review of existing security standards and assessment frameworks, with a particular focus on NIST's (National Institute of Standards and Technology) special publications on security techniques, including those still under development. By analysing their strengths, weaknesses, and areas of focus, the study identifies which frameworks are most suited for IoT-based smart environments. Additionally, it evaluates the practical application of these frameworks in real-world scenarios, examining their ability to uncover vulnerabilities, assess security postures, and guide the implementation of effective countermeasures. The findings highlight that while traditional security frameworks may not fully address the unique challenges of IoT environments, they can be adapted to meet these needs. This paper provides insights for researchers, industry practitioners, and policymakers and paves the way for future research to develop tailored security standards and frameworks. It also discusses the key challenges facing IoT security and offers a roadmap for advancing the safe, secure, and sustainable deployment of IoT technologies.

Keywords— Internet of Things, big data, IoT-enabled Smart Environments, IoT Security, Security Postures, Tailored Frameworks

INTRODUCTION

The Internet of Things (IoT) is a relatively new and rapidly evolving technology that continues to gain traction across diverse industries. According to [1], the Internet of Things (IoT) has had a revolutionary impact in many areas of our daily lives. It has emerged as a crucial enabler of innovation and success across multiple sectors, particularly in the development of innovative environments powered by IoT technologies [2]. In fact IoT has emerged as a crucial enabler of innovation and success across multiple sectors, particularly in the development of innovative smart city environments powered by IoT technologies [2, 3].

Despite these advancements, the connectivity that defines IoT also introduces significant security risks. The devices within these systems, along with the data they sense, collect, and transmit, are highly susceptible to cyber threats. Each connected device presents a potential vulnerability—an entry point for malicious actors. This reality underscores the pressing need for rigorous security assessments and hardening measures in IoT-enabled smart environments.

Although IoT is expected to continue influencing various aspects of our future lives [4, 5], the technology is also accompanied by persistent security and privacy concerns. These challenges are exacerbated by the dynamic, heterogeneous, and often opaque nature of smart IoT environments. Conducting effective security assessments becomes particularly difficult in settings where network posture, visibility, or the security landscape is uncertain.

The situation is further complicated by the limited professional support available for most interconnected IoT devices. Once deployed, many of these devices provide little to no ongoing assistance in their design or operational phases [1]. This lack of support directly impacts the ability to address essential security and privacy needs in IoT- based smart ecosystems.

Despite the increasing adoption of IoT technologies, there remains a significant gap in comprehensive security frameworks tailored to their unique challenges. Traditional security standards often fail to address the dynamic and heterogeneous nature of IoT ecosystems, which involve diverse devices, communication protocols, and decentralized architectures. While organizations such as the National Institute of Standards and Technology

(NIST) have developed security guidelines, their applicability to IoT environments requires further examination.

- *Research Objectives*

This study aims to bridge this gap by conducting an extensive review of existing security standards and assessment frameworks, with a particular focus on NIST's special publications on security techniques including those still under development. The objective is to evaluate their suitability for IoT-based smart environments, identify strengths and weaknesses, and determine their practical effectiveness in real world deployments.

- *Research Questions*

To achieve this objective, the study addresses the following key research questions:

1. What are the most prominent security standards and frameworks applicable to IoT-based smart environments?
2. How well do existing security frameworks (particularly NIST's guidelines) address the unique challenges of IoT security?
3. What practical insights can be derived from real-world implementations of these frameworks in IoT security assessments?

LITERATURE REVIEW

Capacity-building via open educational resources can accelerate practitioner upskilling for IoT security [6], while AI adoption patterns in SMEs highlight practical constraints and adoption pathways relevant to smart environments [7].

As summarized in Table I, widely-used frameworks (NISTIR 8228, NISTIR 8259, ISO/IEC 27001, ENISA) cover complementary layers of IoT risk. The common gaps motivate layered defenses illustrated in Fig. 1. Foundational guidelines such as NISTIR 8228 highlight lifecycle risks [8]. For device manufacturers, NISTIR 8259 defines baseline capabilities [9]. In parallel, NIST SP 800-53 Rev.5 provides a comprehensive catalog of security controls [10].

TABLE I. COMPARISON OF MAJOR DSECURITY
FRAMEWORKS FOR IoT

Framework	Publisher	IoT Focus	Strengths	Gaps/Limitations
NISTIR 8228 (2019)	NIST	Risk mgmt & lifecycle	Clear org guidance	Not device-specific controls
NISTIR 8259 (2020)	NIST	Device manufacturer	Device capabilities baseline	Voluntary; adoptior varies
NIST SP 800-53 Rev.5 (2020)	ISO/IEC	Enterprise controls	Comprehensive control catalog	Tailoring needed foı
ISO/IEC 27001:2022	ENISA	ISMS	Certification-ready	Indirect IoT coverag
ENISA IoT Baselines (2017)	NIST	Critical IoT	Actionable baseline	Dated; needs updat

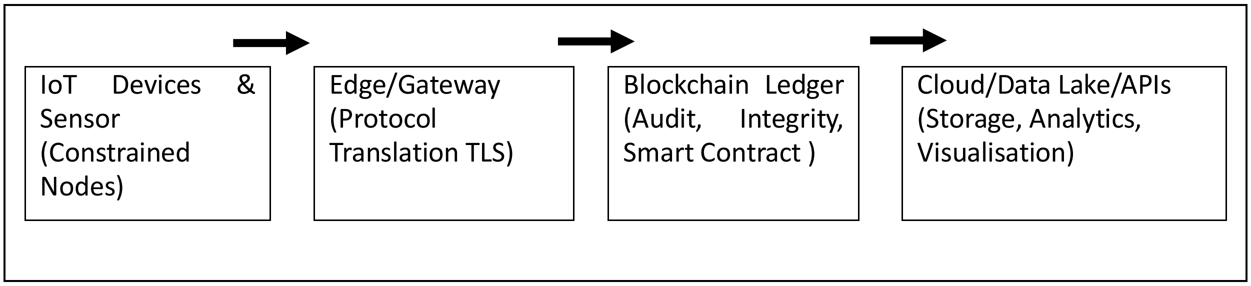

IoT Devices & Sensor (Constrained Nodes)
Edge/Gateway (Protocol Translation TLS)
Blockchain Ledger (Audit, Integrity, Smart Contract)
Cloud/Data Lake/APIs (Storage, Analytics, Visualisation)

Fig. 1. IoT-enabled smart environment security architecture

The security of IoT-enabled smart environments especially smart cities has attracted substantial attention because these systems combine heterogeneous devices, multiple stakeholders, and high-value services. Research falls into three overlapping areas: (1) proposed architectures and platforms for secure IoT communication, (2) mechanisms for data governance and access control, and (3) framework-level studies that identify threats and recommend security designs for city-scale deployments.

- *IoT and decentralized platforms for smart environment*

Several studies propose IoT-based platforms to secure communication and services in smart cities. For example, [11] introduces Orthus, a blockchain platform designed to secure inter-city data and service exchanges; the work outlines required components, operational workflows, and how blockchain primitives can mitigate tampering and unauthorized access. Blockchain solutions are attractive because they provide tamper-evidence, decentralized identity, and auditable logs; however, they also raise throughput, latency, and storage-cost concerns for resource-constrained IoT environments.

- *Data governance, integrity, and access control*

Data governance is a recurring theme. In [12] they argue that smart technologies create new demands around storage, governance, and regulated access to information. That work proposes SmartPrivChain, a hybrid approach combining access control with auditable data-audit mechanisms to secure data sharing across stakeholders. The paper highlights the need to regulate *who* can access what data and for what purpose, a requirement that is especially critical in multi-stakeholder smart-city contexts (e.g., utilities, transport, healthcare).

→

- *Threat identification and privacy-preserving communication frameworks.*

Research summarized in [13] stresses that modern cities prioritize efficiency and quality-of-life gains through technology but remain highly vulnerable to heterogeneous security threats. The study catalogs probable attack vectors (e.g., data exfiltration, device hijacking) and argues for communication frameworks that differentiate between public and private data flows, enforcing privacy, integrity, and confidentiality according to data sensitivity. This work supports a design philosophy of context-aware security controls rather than one-size-fits-all solutions.

- *Distributed verification and P2P techniques to reduce cost and increase trust.*

Li's work [2] emphasizes three practical barriers for smart cities: insecure IoT endpoints, high costs for centralized data center storage, and limited end-user privacy. Li proposes using P2P distributed storage and cryptographically enforced validation and consensus to (a) reduce central storage costs and (b) validate genuine IoT nodes to prevent rogue devices from joining the network. This approach shows promise for reducing operational costs and bolstering trust, but it also brings new challenges in ensuring timely consensus and protecting availability.

- *Synthesis of Findings*

Across the surveyed works, several themes emerge:

1. Security-by-design principles are necessary for IoT-enabled smart environments.
2. Decentralized approaches such as blockchain and P2P improve auditability but are resource-intensive for constrained devices.
3. Fine-grained governance of data access and retention is critical where multiple entities share information.
4. Many studies remain at the architectural or prototype stage, with limited real-world evaluations.

or you.

- *Issues And Challenges*

Compliance with ISO/IEC 27001:2022 offers a certification-ready ISMS, though its IoT coverage remains limited [14]. From a European perspective, ENISA's IoT Baselines provide actionable recommendations for critical infrastructures [15].

Capacity building through open educational resources can accelerate training of IoT security practitioners [6]. Lessons from AI adoption in Zambian SMEs demonstrate pathways for innovation and sustainability in IoT-smart environments [7].

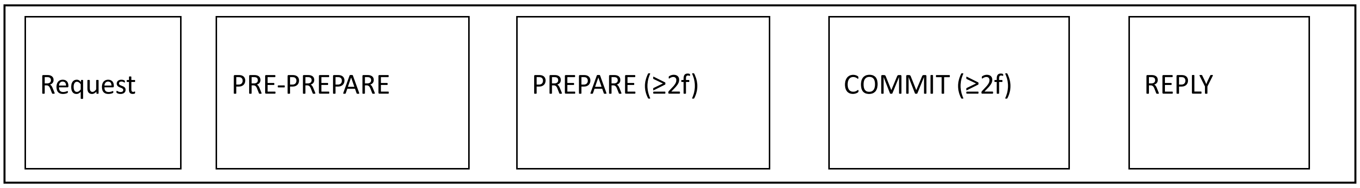
Smart cities are underpinned by extensive technological infrastructures and continuous streams of heterogeneous data that must operate concurrently and reliably to ensure the stability of urban systems [16]. The failure of critical subsystems poses significant risks, as even localized disruptions can precipitate systemic consequences. For instance, environmental and traffic sensors are deployed to monitor parameters such as temperature, humidity, wind speed, and vehicular flow. A malfunction of traffic management infrastructure—such as traffic lights and surveillance systems—could result in severe congestion, heightened accident rates, and the consequent obstruction of emergency response services.

As shown in Fig. 2, the consensus pipeline ensures safety by requiring quorum thresholds (≥2f) for PREPARE and COMMIT phases before a REPLY is issued.

Methodology

- *System Architecture and Operations*

To illustrate how the system operates in practice, consider a specific sub-system within the broader smart city infrastructure namely, the *IoT-based parking allocation system* [13]. This example demonstrates how blockchain and IoT layers interact to provide secure, transparent, and efficient services to city residents.



1. *Block Approval:* When a user requests a parking spot, the system processes the request through one of the IoT gateways. The interface layer handles the request, determines the optimal parking location, and issues this information to the user. Simultaneously, the transaction is recorded on the blockchain ledger as the latest entry, ensuring traceability and security.
2. *Spot Reservation:* Once the parking spot is identified, it must be reserved for the user. The system assigns a sequence number and links it to the most recent blockchain entry. This finalizes the reservation, and the system updates its status to indicate that the spot is reserved.

- *IoT consensus protocols*

To achieve consensus and maintain the integrity of reservations, the system applies IoT consensus protocols. The following pseudocode outlines the process for parking spot reservation [2, Algorithm 1]:

Algorithm 1: Parking Spot Reservation for User *i*

Input: Parking request from user i
Output: Confirmation of reserved parking spot

```
Step 1: Request Handling
while user_i receives valid_request = True do
  if user_identity_authentication = True then
    m ← request
    multicast PRE-PREPARE message to other members
  end if
end while

Step 2: Prepare Phase
while user_i receives valid_prepare = True do
  if number_of_valid_prepare > 2f then
    multicast COMMIT message to other members
  end if
end while

Step 3: Commit Phase
while user_i receives valid_commit = True do
  if number_of_valid_commit > 2f then
    send REPLY message to the client
  end if
end while
```

Fig. 2 Lightweight consensus sequence for IoT parking-slot allocation

- *consensus process and authenticated requests Specifications*

This consensus process ensures that only authenticated requests are considered, transactions are validated by multiple network participants, and the final confirmation is securely logged on the blockchain. In this way, fraudulent or conflicting parking requests are detected and prevented, guaranteeing both transparency and fairness in the system.

Discussions

All nodes in the system maintain identical copies of the blockchain, enabling the detection of unauthorized or unwanted requests with relative ease [7, 12]. A malicious node cannot arbitrarily request a block, as all submissions are bound to their respective positions within the chain. Similarly, malicious activities such as attempting to reserve multiple parking spaces simultaneously are quickly identified, since all nodes access and validate transactions against the same distributed ledger in real time.

In cases where the reservation process fails, the system incorporates a retry mechanism. The user may attempt the reservation again after a predefined countdown period. If the parking space has not already been allocated to another user, the same sequence number can be reused to complete the transaction. This approach ensures fairness, prevents duplication, and maintains the integrity of the allocation process.

FINDINGS

The analysis of IoT-enabled smart environments highlighted several key findings. Firstly, traditional security standards such as ISO 27001 and NIST CSF offer strong foundations but lack coverage of heterogeneous IoT ecosystems. Practical IoT deployments in agriculture demonstrate how microcontroller-based sensing and actuation can inform broader smart environment designs [16].

Secondly, blockchain-based approaches improve auditability and trust but introduce resource and latency constraints. Thirdly, access control and data governance frameworks such as SmartPrivChain demonstrate promising results in multi-stakeholder environments. Finally, real-world deployments remain limited, emphasizing the need for further empirical validation.

RECOMMENDATIONS

Based on the findings, this study recommends the following:

i. Adoption of hybrid security frameworks that integrate blockchain and NIST guidelines.

ii. Implementation of security-by-design principles during IoT device development.

iii. Stronger collaboration between academia, industry, and regulators to define interoperable standards.

iv Development of lightweight consensus protocols optimized for resource-constrained devices.

v. Enhanced training programs for practitioners to manage IoT ecosystems securely.

FUTURE WORK

Future research should focus on developing standardized, interoperable frameworks that can adapt to heterogeneous IoT ecosystems. Emphasis should be placed on incorporating artificial intelligence and machine learning models for real-time anomaly detection and automated response. Another area of future work lies in creating benchmark datasets for IoT security evaluation. Additionally, pilot projects in smart cities will be critical to test, refine, and validate proposed frameworks at scale.

CONCLUSION

Technology presents significant potential in the context of smart cities, particularly as a foundation for secure and resilient IoT-enabled environments. This paper has proposed a security framework that leverages a blockchain-based database to support multiple subsystems, such as parking allocation and access control. The key advantage of blockchain lies in its inherent resistance to tampering, ensuring that data cannot be manipulated without proper authorization. This makes it especially valuable in smart city infrastructures where transparency, integrity, and trust are paramount.

As urbanization accelerates, cities are increasingly challenged by issues such as congestion, financial pressures, and resource distribution. A blockchain-enabled IoT framework offers a promising pathway to address these challenges by facilitating equitable access to resources, enabling seamless data sharing, and supporting real-time decision-making across diverse subsystems. Importantly, the decentralized ledger ensures that stakeholders can access relevant information easily while maintaining privacy protections and safeguarding against malicious activities.

Furthermore, advances in networking technologies providing faster speeds, greater reliability, and support for a wider range of devices make it feasible to integrate blockchain with IoT systems at scale. This integration supports not only conventional data but also multimedia and complex transactional processes.

Looking ahead, the development of interoperable and scalable frameworks will be crucial. Future research should focus on evaluating and standardizing security models that can operate across heterogeneous IoT devices and services while ensuring efficiency and sustainability. By doing so, blockchain-based security frameworks can serve as a cornerstone in the creation of smart cities that are not only technologically advanced but also secure, transparent, and equitable.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer

Networks, vol. 54, no. 15, pp. 2787–2805, 2010. doi:10.1016/j.comnet.2010.05.010

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013. doi:10.1016/j.future.2013.01.010

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, Feb. 2014. doi:10.1109/JIOT.2014.2306328

[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146–164, 2015. doi:10.1016/j.comnet.2014.11.008

[5] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013. doi:10.1016/j.comnet.2012.12.018

[6] J. Egan, T. Frindt, and J. Mbale, "Open Educational Resources and the Opportunities for Expanding Open and Distance Learning (OERS-ODL)," International Journal of Emerging Technologies in Learning (iJET), vol. 8, no. 2, pp. 57–64, 2013. doi:10.3991/ijet.v8i2.2312

[7] R. Phiri and J. Mbale, "Leveraging Machine Learning and Artificial Intelligence for Innovation and Sustainability in Small and Medium Sized Enterprises (SMEs): A Case Study of Kalumbila, Zambia," Proc. ICICT-Zambia, vol. 6, no. 1, pp. 56–62, 2024.

[8] K. Boeckl et al., "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," NISTIR 8228, NIST, 2019. doi:10.6028/NIST.IR.8228

[9] M. Fagan et al., "Foundational Cybersecurity Activities for IoT Device Manufacturers," NISTIR 8259, NIST, 2020.

[10] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53 Rev. 5, Sep. 2020 (incl. Dec. 2020 updates). doi:10.6028/NIST.SP.800-53r5

[11] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLOS ONE, 11(10): e0163477, 2016. doi:10.1371/journal.pone.0163477

[12] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," Proc. 3rd USENIX OSDI, 1999, pp. 173–186.

[13] A. Khanna and R. Anand, "IoT based Smart Parking System," Proc. 2016 Int. Conf. Internet of Things and Applications (IOTA), 2016, pp. 266–270. doi:10.1109/IOTA.2016.7562735

[14] ISO/IEC 27001:2022, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," ISO/IEC, 2022.

[15] ENISA, "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures," European Union Agency for Cybersecurity, 2017.

[16] J. Kalezhi, J. Mbale, and L. Ndovi, "Microcontroller-Based Monitoring and Controlling of Environmental Conditions in Farming," 2018 IEEE PES/IAS PowerAfrica, 2018, pp. 284–288. doi:10.1109/PowerAfrica.2018.8521055