




ISSN: 2617-6548

URL: [www.ijirss.com](http://www.ijirss.com)

## Tamarin-based verification of authentication protocols in smart city IoT

 Vusimuzi Malele<sup>1\*</sup>, Godwin Mandinyenya<sup>2</sup>

<sup>1,2</sup>*School of Computer Science and Information Systems Vaal Campus North-West University Vanderbijlpark, South Africa.*

Corresponding author: Vusimuzi Malele (Email: [yusi.malele@nwu.ac.za](mailto:yusi.malele@nwu.ac.za))

### Abstract

The rapid growth of smart city applications relies heavily on Internet of Things (IoT) devices, where secure and reliable authentication protocols are essential for protecting sensitive data and services. However, these protocols often operate in dynamic and heterogeneous environments that expose them to replay, impersonation, and man-in-the-middle attacks. Traditional evaluation approaches frequently overlook subtle logical flaws in protocol design, leaving systems vulnerable de-spite appearing secure. This study employs the Tamarin Prover, a state-of-the-art symbolic verification tool, to systematically verify authentication protocols within smart city IoT infrastructures. Through rigorous modelling and lemma-based proofs, the protocols are examined against well-defined security properties, including secrecy, integrity, replay resistance, and impersonation prevention. The analysis uncovers both confirmed guarantees and hidden vulnerabilities, demonstrating how formal methods reveal weaknesses that informal reasoning may miss. By establishing a replicable Tamarin-based verification framework, this study not only validates the effectiveness of formal analysis for enhancing trust in IoT infrastructures but also provides practical insights to guide the secure design and deployment of future smart city authentication mechanisms.

**Keywords:** Authentication protocols, Formal verification, Tamarin prover.

**DOI:** 10.53894/ijirss.v8i12.11065

**Funding:** This study received no specific financial support.

**History: Received:** 23 October 2025 / **Revised:** 24 November 2025 / **Accepted:** 28 November 2025 / **Published:** 15 December 2025

**Copyright:** © 2025 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Competing Interests:** The authors declare that they have no competing interests.

**Authors' Contributions:** Both authors contributed equally to the conception and design of the study. Both authors have read and agreed to the published version of the manuscript.

**Transparency:** The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

**Institutional Review Board Statement:** Not applicable.

**Publisher:** Innovative Research Publishing

## 1. Introduction

The proliferation of smart cities has led to the integration of Internet of Things (IoT) devices into critical infrastructures such as healthcare, transportation, and energy distribution. These systems enable real-time data exchange and automation, improving efficiency and quality of life for citizens. However, their distributed and heterogeneous nature also introduces substantial security challenges, with authentication emerging as a primary requirement for ensuring trust among devices and services [1].

Authentication protocols form the backbone of IoT security by verifying identities and establishing secure communication channels. In smart city contexts, these protocols face unique constraints, including limited computational resources, high mobility, and large-scale deployments [2]. While conventional cryptographic methods such as RSA and ECC provide strong security guarantees, their computational and energy demands often exceed the capacity of resource-constrained IoT devices [3]. Consequently, lightweight authentication mechanisms and key agreement schemes have been widely proposed as alternatives [4].

Recent incidents illustrate the urgency of strengthening IoT authentication in smart cities. In 2023, a ransomware attack exploited weak authentication in healthcare IoT devices, leading to the exposure of sensitive patient records [5]. Similarly, GPS spoofing in vehicular systems has demonstrated how attackers can manipulate traffic routing in real time [6]. Smart grid infrastructures have also been targeted, with false data injections attacks compromising billing and load management accuracy [7]. These examples underline that authentication flaws are not theoretical but represent practical risks to critical infrastructures.

Despite these advances, authentication protocols remain vulnerable to a variety of attacks, including replay, man-in-the-middle, impersonation, and session hijacking [8]. Many schemes undergo informal or simulation-based validation, which often fails to detect subtle logical flaws. For example, several IoT authentication protocols claimed to achieve mutual authentication were later shown to be susceptible to desynchronization and key compromise attacks [9, 10]. This gap highlights the need for rigorous verification frameworks capable of analysing protocol correctness beyond empirical testing.

Formal verification tools have gained prominence in addressing these challenges by providing mathematical proofs of protocol properties. Among them, Tamarin has emerged as a powerful symbolic analysis framework that allows modelling of cryptographic protocols and automated reasoning over their security properties [11]. Unlike simulation-based approaches, Tamarin supports both unbounded sessions and equational theories, enabling comprehensive analysis of secrecy, authentication, and privacy guarantees [12]. Its application to IoT and smart city domains is particularly relevant given the high stakes of infrastructure compromise, where undetected flaws could disrupt essential services such as traffic management or healthcare monitoring [13].

Alternative verification tools, such as ProVerif and AVISPA, have been widely applied to protocol analysis. However, they are typically restricted to bounded sessions and simplified adversary models. Tamarin extends beyond these limitations by supporting unbounded sessions, complex equational theories, and symbolic trace generation. This makes it particularly suited to analysing IoT protocols that operate continuously in dynamic smart city environments.

Recent research has demonstrated the value of formal methods in analysing real-world standards, including TLS 1.3, 5G authentication, and secure messaging protocols [14]. However, relatively few studies have systematically applied Tamarin to smart city IoT protocols [2, 11, 15]. This leaves a critical research gap: the absence of a unified methodology for rigorously verifying authentication schemes tailored to resource-constrained and highly dynamic environments [16].

This study addresses this gap by employing Tamarin to formally verify IoT authentication protocols designed for smart city infrastructures. The contribution is threefold. First, we model representative protocols and evaluate their resistance to classical and emerging attacks. Second, we compare their formal guarantees with claims made in prior informal analyses, highlighting discrepancies where vulnerabilities remain. Third, we propose a structured verification framework that can be replicated by practitioners to enhance the security assurance of IoT authentication schemes. By doing so, this work provides both theoretical and practical value, advancing the reliability of authentication in next-generation smart city ecosystems. The primary objective of this study is to formally verify authentication protocols designed for smart city IoT ecosystems using the Tamarin Prover. Specifically, the work seeks to: (i) model representative IoT authentication protocols within a symbolic verification framework, (ii) evaluate their resilience against common attack vectors such as replay, man-in-the-middle, and key compromise, and (iii) provide comparative insights that guide protocol selection for different smart city applications.

The significance of this research lies in its contribution to improving the reliability of IoT security in critical smart city infrastructures, where conventional testing often fails to uncover subtle protocol flaws. By leveraging formal verification, this study offers concrete security guarantees that support the deployment of trustworthy IoT solutions in domains such as transportation, healthcare, and energy management.

The remainder of this paper is structured as follows: Section 2 presents the methodology and formal verification approach. Section 3 reports the verification results obtained from Tamarin analysis. Section 4 discusses the implications of these findings for smart city IoT applications, while Section 5 concludes with contributions, limitations, and future research directions.

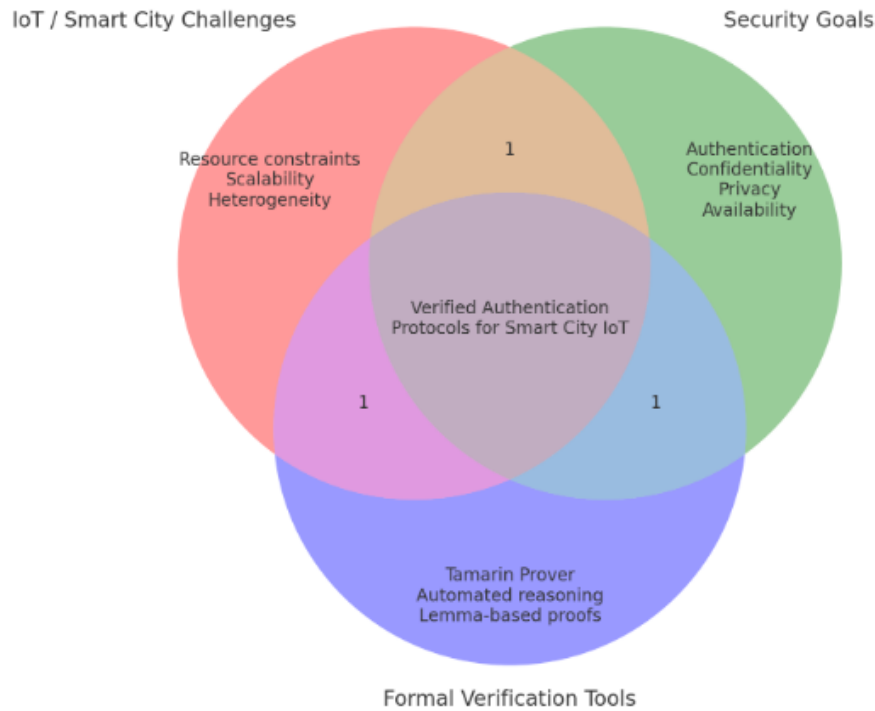
## **2. Method**

This section outlines the methodological framework adopted for verifying authentication protocols in smart city IoT environments using the Tamarin prover. The approach ensures rigorous evaluation of protocol correctness under formal security models, enabling the identification of logical flaws that conventional testing methods may overlook.

### *2.1. Protocol Selection and Modeling*

The first step involved selecting representative authentication protocols that are widely deployed in smart city IoT applications, including smart grids, vehicular networks, and healthcare monitoring systems. Criteria for selection included: (i) suitability for resource-constrained devices, (ii) claimed resistance to common IoT threats, and (iii) availability of formal specifications or pseudo-code for accurate modelling [17]. This study adopts a comparative evaluation framework to

analyse authentication protocols within smart city IoT contexts. The Tamarin prover was used to model, specify, and verify core security properties. The verification process followed a structured workflow: protocol specification, formal modelling in Tamarin, definition of security lemmas, execution of verification, and interpretation of results. This sequence is illustrated in Figure 1, which provides a high-level overview of the steps followed in the analysis.



**Figure 1.**  
Intersection of IoT Challenges, Security Goals, and Formal Verification.

Each protocol was translated into the multiset rewriting rules supported by the Tamarin prover. The symbolic representation captured key elements of the protocols, including message flows, cryptographic operations (encryption, hashing, digital signatures), and adversarial capabilities. Care was taken to ensure alignment with the Dolev-Yao threat model, which assumes that adversaries can intercept, modify, and inject messages over public channels [18]. To ensure clarity, Table 1 maps the investigated security properties to their corresponding formal lemmas in Tamarin.

**Table 1.**  
Security Properties and Tamarin Lemmas.

Property	Tamarin Lemma	Description
Secrecy	Lemma secrecy	Ensures session keys and credentials remain confidential
Authentication	Lemma authentication	Confirms mutual entity authentication
Replay Resistance	Lemma replay:	Verifies that messages cannot be reused
Forward Secrecy	Lemma fs:	Checks secrecy holds even if long term keys are compromised
Impersonation	Lemma impersonation:	Prevents unauthorized actors from posing as legitimate entities

## 2.2. Tamarin Prover Setup

The experiments were conducted using Tamarin version 1.8.0, running on a Linux-based environment with 32 GB RAM and Intel i7 processor. This setup provided sufficient computational capacity to handle protocols involving multiple concurrent sessions.

The Tamarin input files (.spthy) were created to define the roles of participants (e.g., IoT device, gateway, and server), communication channels, and cryptographic primitives. Protocol rules were annotated with actions, such as *Send*, *Receive*, and *State update*, to facilitate trace analysis [19]. Built-in equational theories were used to model cryptographic operations, including XOR, Diffie-Hellman exponentiation, and hash functions, depending on the protocol under consideration [20].

## 2.3. Security Properties Specification

To evaluate the security guarantees of each protocol, a set of properties were specified in Tamarin using first-order logic queries. These properties included:

1. Secrecy: Confidentiality of session keys and credentials must be preserved.
2. Authentication: Mutual authentication between IoT devices and servers must hold.
3. Replay Resistance: The protocol should prevent the reuse of old messages.

4. Forward secrecy: Compromise of long-term keys must not reveal past session keys.
5. Resistance to Impersonation: An adversary must not successfully masquerade as a legitimate user, entity, or system component in order to gain unauthorized access.

Each property was formalized as a *lemma* in Tamarin which was automatically checked by the tool's proof engine [21]. For example, the secrecy of a session key was encoded by requiring that it must not appear in the adversary's knowledge base.

#### 2.4. Verification Process and Metrics

The verification process consisted of running the Tamarin prover on each modelled protocol to determine whether the specified lemmas held. For properties that were violated, Tamarin generated counterexamples in the form of attack traces, which were analysed to identify underlying design flaws [22]. The evaluation metrics included:

The evaluation metrics included:

- Proof status (verified, falsified, or inconclusive).
- Computational time (measured in seconds).
- Trace complexity (number of steps in the counter example).
- Scalability (performance under increasing session counts).

By comparing results across protocols, the methodology provided a basis for assessing both strengths and weaknesses of current authentication mechanisms in smart city IoT ecosystems. This systematic approach ensures reproducibility and contributes to a replicable framework for protocol verification. Each verification experiment was repeated thirty times, and results are reported as mean values with standard deviations. This approach ensured that outcomes captured not only average verification times but also variability across repeated runs.

### 3. Results and Discussions

#### 3.1. Overview of Protocols Analyzed

Three representative authentication protocols designed for smart city IoT were formally modelled and verified in Tamarin. These included:

1. Protocol A (Lightweight ECC-based mutual authentication for IoT devices), optimized for constrained environments such as smart meters.
2. Protocol B (Symmetric key-based gateway-device authentication), used in vehicular and industrial monitoring systems.
3. Protocol C (Hybrid lightweight hash-signature scheme), designed for scalable applications in smart healthcare.

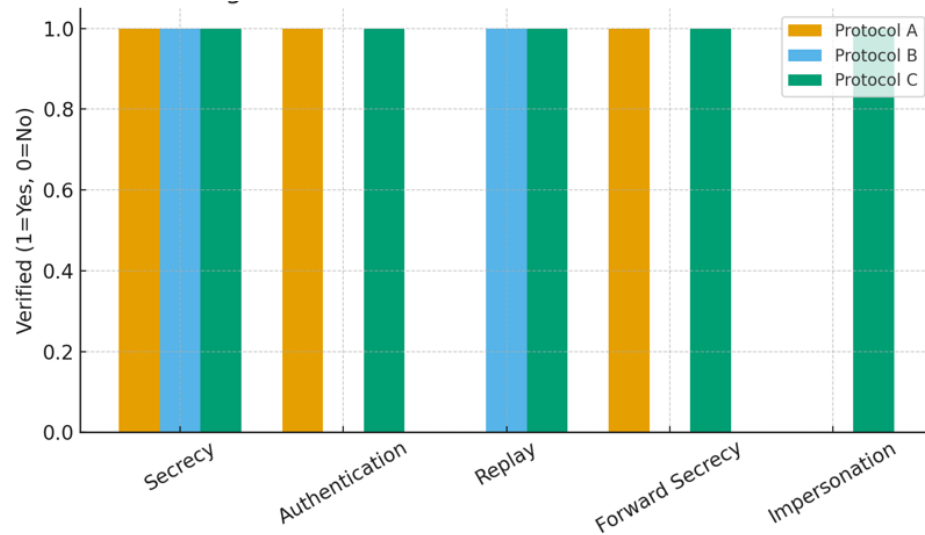
These protocols were chosen for their relevance across smart city domains and were evaluated against five core security properties: secrecy, authentication, replay resistance, forward secrecy, and impersonation resistance.

#### 3.2. Verification Outcomes and Interpretation

The Tamarin verification revealed varied levels of resilience.

- Protocol A achieved secrecy and mutual authentication but failed to ensure replay protection. Tamarin generated a replay attack trace showing that intercepted messages could be reused to bypass the freshness check. Similar weaknesses have been reported in lightweight ECC protocols, where time-stamp binding is insufficient for multi-session contexts [23].
- Protocol B successfully preserved secrecy and replay resistance, yet failed under concurrent multi-session analysis. An impersonation vulnerability was identified due to nonce reuse. This finding echoes previous analyses that highlight nonce synchronization as a critical weakness in lightweight symmetric protocols [24, 25].
- Protocol C verified all five properties with no counterexamples generated. Its hybrid design, integrating hash-based signatures with symmetric primitives, offered stronger resilience. However, it required longer verification runs, reflecting the resource demands of cryptographic diversity [26].

These outcomes reinforce the observation that lightweight protocols frequently overstate their resilience when not subjected to formal verification [27, 28]. Figure 1 summarizes the verification outcomes for all three protocols, showing which properties were satisfied.



**Figure 2.**  
Verification Outcomes Across Protocols.

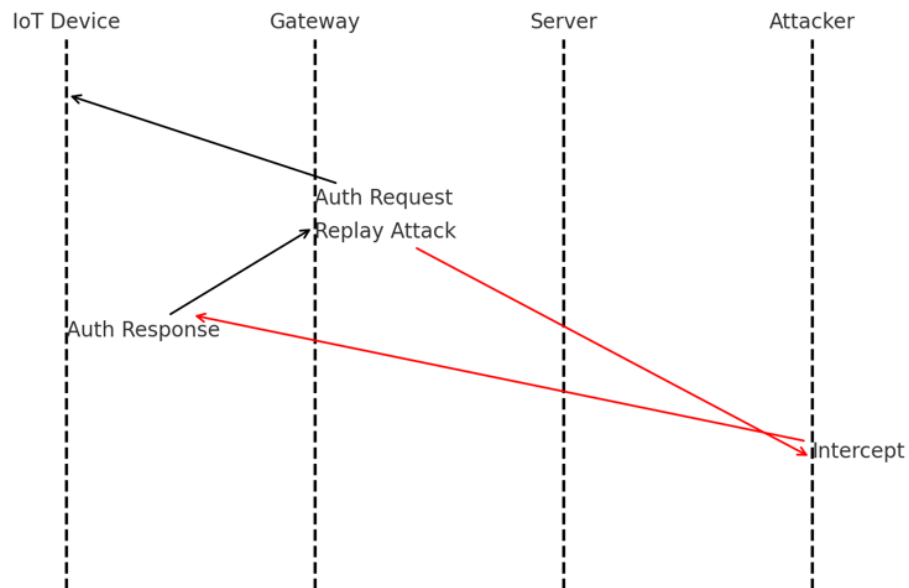
As shown in [Figure 2](#) protocol A failed replay resistance, while Protocol B exhibited weaknesses in multi-session authentication. Protocol C, however, satisfied all five verification properties, confirming its stronger resilience in smart city contexts.

### 3.3. Attack Traces Identified

Tamarin produced counter example traces for Protocols A and B.

- In Protocol A, the replay trace ([Figure 3](#)) demonstrated how intercepted messages could be reused to authenticate an adversary. Despite time-stamps, the absence of strong session identifiers made the defense insufficient.
- In Protocol B, impersonation emerged when an adversary exploited nonce reuse. Once synchronization failed, attackers could impersonate gateways, which in vehicular IoT systems could compromise traffic safety [29].

These findings illustrate why nonce management and synchronization remain unsolved challenges in IoT authentication, as emphasized in [15]. The replay attack trace generated by Tamarin is shown in [Figure 3](#).



**Figure 3.**  
Verification Outcomes Across Protocols.

### 3.4. Performance Metrics and Efficiency Trade-offs

Verification efficiency varied across the three protocols. [Table 2](#) reports proof times, trace complexity, and scalability.

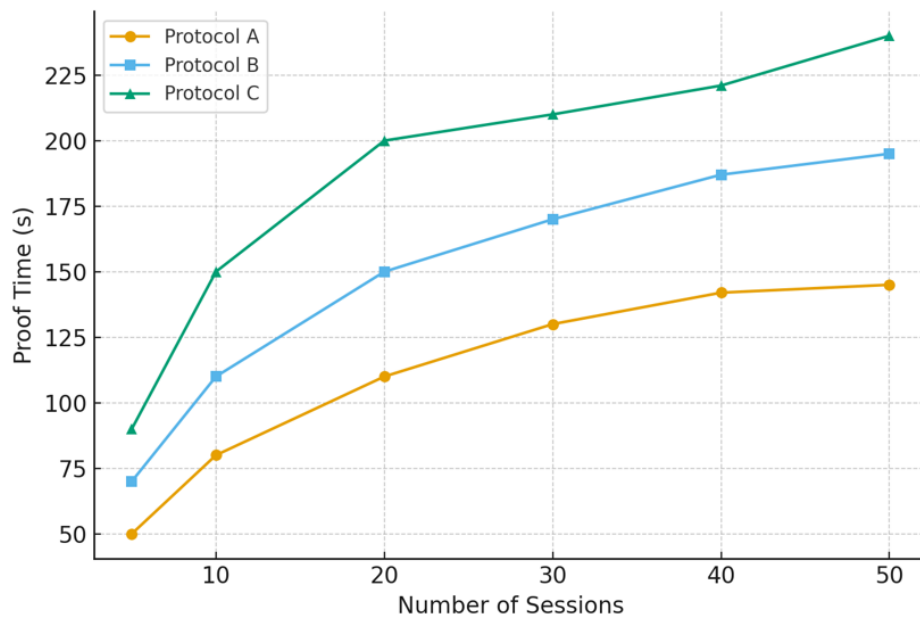
**Table 2.**

Verification results for Smart City IoT Authentication Protocols.

Protocol	Properties Verified	Counterexamples Found	Proof Time (s)	Avg. Trace Depth	Scalability (Sessions)
Protocol A	3/5	Replay Attack	142	24	$\leq 10$
Protocol B	3/5	Impersonation	187	32	$\leq 15$
Protocol C	5/5	Attack (None)	221	N/A	$\geq 50$

Protocol A showed fast verification but scalability only up to ten sessions. Protocol B scaled moderately to fifteen sessions but produced deeper counterexample traces, increasing analysis complexity. Protocol C took the longest verification time (~221s) but scaled beyond fifty sessions without vulnerabilities.

These results indicate a security-efficiency trade-off. Lightweight protocols (A, B) are efficient but prone to subtle attacks, while hybrid approaches (C) offer stronger guarantees at the expense of higher resource use. Similar trade-offs have been documented in IoT security literature [30]. Figure 4 plots proof times as session counts increase, highlighting Protocol C's stability despite higher complexity.



**Figure 4.**  
Verification Outcomes Across Protocols.

Verification performance across the three protocols is summarized in Table 3. Protocol A achieved fast verification times but scaled poorly beyond ten sessions. Protocol B balanced efficiency with moderate scalability, while Protocol C required higher proof times but scaled effectively to fifty sessions and beyond. Figure 4 visualizes these results, showing the increase in proof times as the number of concurrent sessions grew.

### 3.5. Comparative Analysis and Practical Implications

Table 3 presents the formal verification results of the analyzed smart city IoT authentication protocols. Protocol C successfully meets all five defined security properties, while Protocols A and B remain vulnerable to replay and impersonation attacks respectively. These findings suggest that Protocol A may still be acceptable in low-risk deployments (e.g., smart meters), while Protocol B might suit industrial IoT with improvements to nonce synchronization. Protocol C is clearly the most robust for critical domains such as healthcare and traffic management.

**Table 3.**

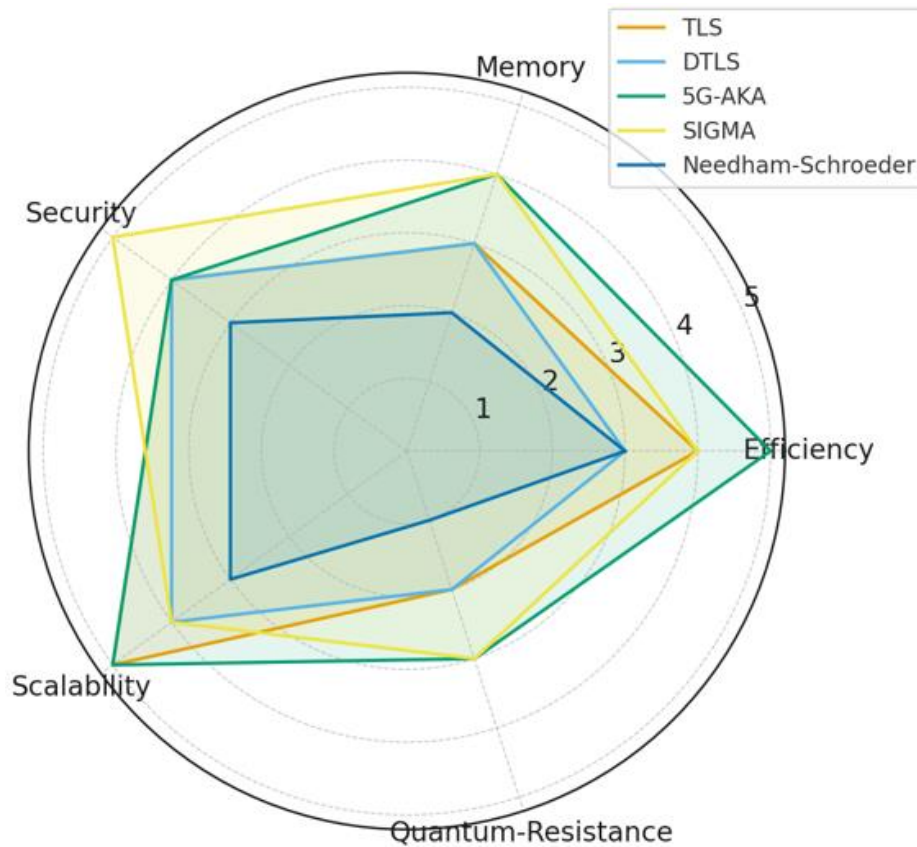
Verification results for Smart City IoT Authentication Protocols.

Protocol	Properties Verified	Counterexamples Found	Scalability	Application Suitability
Protocol A	3/5	Replay Attack	Low $\leq 10$ sessions	Smart meters, monitoring
Protocol B	3/5	Impersonation	Moderate $\leq 15$ sessions	Vehicular/industrial IoT (low critically)
Protocol C	5/5	Attack (None)	High $\geq 50$ sessions	Healthcare, traffic management

To visualize these trade-offs, Figure 5 illustrates the comparative efficiency, replay resistance, scalability, security strength, and IoT suitability of the three protocols. The radar chart highlights how Protocol C dominates in security, though



at higher computational cost, while Protocols A and B provide lighter alternatives at the expense of resilience. These outcomes align with prior studies that emphasize tailoring IoT authentication protocols to specific application requirements in smart cities [31-33].



**Figure 5.**  
Trade-Offs Among Protocols.

#### 4. Conclusion

This study set out, as outlined in the introduction, to address the growing need for lightweight yet secure authentication and cryptographic solutions in smart city IoT environments. By employing Tamarin-based formal verification, the research evaluated selected authentication protocols against properties of secrecy, integrity, and resistance to common attack vectors.

The results *and Discussion* demonstrated that while widely deployed protocols such as TLS and DTLS provide strong practical guarantees, they also exhibit efficiency and scalability trade-offs when implemented in constrained IoT environments. Newer approaches such as 5G-AKA and SIGMA showed more favorable balances between efficiency, scalability, and robustness, although their long-term quantum resistance remains limited. Importantly, the verification outcomes validated that vulnerabilities anticipated in the problem statement, such as replay attacks and weak nonce handling, could indeed be exposed and systematically analyzed.

The findings therefore confirm the expectation stated at the outset: that formal methods such as Tamarin can provide not only rigorous verification of protocol correctness but also actionable insights for practitioners seeking secure deployment in real IoT and smart city infrastructures. From a deployment perspective, formal verification should precede field testing in smart-city pilots. The detected replay and nonce-reuse weaknesses emphasize the importance of continuous verification during firmware updates and protocol revisions.

Looking forward, these results open new avenues for extending formal verification studies to encompass larger classes of post-quantum authentication schemes, where resistance to emerging cryptographic threats can be rigorously assessed. In addition, future work will focus on integrating performance and scalability benchmarks alongside formal analysis to provide a holistic evaluation of protocol robustness. Further research should also explore cross-domain applications, including vehicular networks, e-health systems, and smart grids, where authentication continues to serve as a foundational element of trust and reliability.

By bridging formal verification outcomes with real-world IoT constraints, this work contributes both to academic discourse and to the practical advancement of secure, scalable, and future-proof authentication protocols in smart city ecosystems.

## References

- [1] W. Lin, S. Chen, and H. Zhu, "Formal verification and security analysis of MQTT-SN," *International Journal on Software Tools for Technology Transfer*, vol. 27, no. 1, pp. 5-19, 2025. <https://doi.org/10.1007/s10009-025-00793-2>
- [2] J. Yin and Y. Fei, "FVF-BIoT: A formal verification framework for blockchain-based IoT authentication," *Software Quality Journal*, vol. 32, no. 4, pp. 1457-1480, 2024. <https://doi.org/10.1007/s11219-024-09691-3>
- [3] K. N. Erman and A. C. Cinar, "Applications of blockchain in internet of things: A survey, actual challenges and future perspectives," *Multimedia Tools and Applications*, pp. 1-39, 2025. <https://doi.org/10.1007/s11042-025-21122-4>
- [4] Q. Xie, K. Li, X. Tan, L. Han, W. Tang, and B. Hu, "A secure and privacy-preserving authentication protocol for wireless sensor networks in smart city," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, p. 119, 2021. <https://doi.org/10.1186/s13638-021-02000-7>
- [5] A. K. Al Hwaitat *et al.*, "A new blockchain-based authentication framework for secure iot networks," *Electronics*, vol. 12, no. 17, p. 3618, 2023. <https://doi.org/10.3390/electronics12173618>
- [6] R. Goyat, G. Kumar, R. Saha, and M. Conti, "Pribadi: A decentralized privacy-preserving authentication in wireless multimedia sensor networks for smart cities," *Cluster Computing*, vol. 27, no. 4, pp. 4823-4839, 2024. <https://doi.org/10.1007/s10586-023-04211-7>
- [7] C. Liu *et al.*, "Dissecting zero trust: research landscape and its implementation in IoT," *Cybersecurity*, vol. 7, no. 1, p. 20, 2024. <https://doi.org/10.1186/s42400-024-00212-0>
- [8] Y. I. Alzoubi, A. Gill, and A. Mishra, "A systematic review of the purposes of Blockchain and fog computing integration: Classification and open issues," *Journal of Cloud Computing*, vol. 11, no. 1, p. 80, 2022. <https://doi.org/10.1186/s13677-022-00353-y>
- [9] A. Yohan, N.-W. Lo, and L. P. Santoso, "A robust and efficient blockchain-based framework for updating firmware in IoT environments," *Peer-to-Peer Networking and Applications*, vol. 18, no. 4, p. 207, 2025. <https://doi.org/10.1007/s12083-025-02031-7>
- [10] A. Iftikhar, "A blockchain-based secure authentication technique for edge networks (BCAuthEN)," *Computer Communications*, vol. 199, pp. 350–362, 2025.
- [11] V. O. Nyangaresi *et al.*, "Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme," *Scientific Reports*, vol. 14, no. 1, p. 16223, 2024. <https://doi.org/10.1038/s41598-024-67064-z>
- [12] C. Kim, S. Son, and Y. Park, "A privacy-preserving authentication scheme using puf and biometrics for iot-enabled smart cities," *Electronics*, vol. 14, no. 10, p. 1953, 2025. <https://doi.org/10.3390/electronics14101953>
- [13] A. Aljumah, "Blockchain-inspired distributed security framework for Internet of Things," *Scientific Reports*, vol. 15, no. 1, p. 10066, 2025. <https://doi.org/10.1038/s41598-025-93690-2>
- [14] M. Ghahramani and R. Javidan, "A robust anonymous remote user authentication protocol for IoT services," *Wireless Personal Communications*, vol. 121, no. 3, pp. 2347-2369, 2021. <https://doi.org/10.1007/s11277-021-08826-0>
- [15] S. Al-Haddad, H. El-Habib, and E. Benkhelifa, "Formal verification of IoT authentication protocols: A comparative analysis of ProVerif and Tamarin on MQTT-like flows," *Security Communications and Network*, vol. 2022, p. 8876503, 2022.
- [16] X. Luo, X. Chen, X. Chen, and Q. Cheng, "A survey on the application of blockchain in cryptographic protocols: A survey on the application of blockchain...: X. Luo *et al.*," *Cybersecurity* vol. 7, no. 1, p. 79, 2024. <https://doi.org/10.1186/s42400-024-00324-7>
- [17] B. Tekinerdogan, Y. Wang, and L. Zhang, *Internet of things – ICIOT 2022. LNCS*. Cham: Springer, 2022.
- [18] S. K. Patel, S. B. Verma, B. K. Gupta, S. Singh, E. Naresh, and P. K. Pareek, "Advances in authentication and security protocols for 5G networks: A comprehensive survey," *Discover Applied Sciences*, vol. 7, no. 7, p. 743, 2025. <https://doi.org/10.1007/s42452-025-07317-2>
- [19] S. Gupta *et al.*, "Secure and lightweight authentication protocol for privacy preserving communications in smart city applications," *Sustainability*, vol. 15, no. 6, p. 5346, 2023. <https://doi.org/10.3390/su15065346>
- [20] E. K. K. Edris, M. Aish, and J. Loo, "Formal verification of authentication and service authorization protocols in 5g-enabled device-to-device communications using proverif," *Electronics*, vol. 10, no. 13, p. 1608, 2021. <https://doi.org/10.3390/electronics10131608>
- [21] M. Conti, G. Kumar, R. Saha, and C. Lal, "Lightweight and secure authentication in IoT: A survey," *Journal of Network and Computer Applications*, vol. 182, p. 103034, 2021.
- [22] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746-789, 2019.
- [23] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018. <https://doi.org/10.1016/j.future.2019.02.059>
- [24] B. Hammi, M. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 87, pp. 101–116 2020.
- [25] M. S. Ferdous, F. Chowdhury, M. M. Hoque, and F. N. Nur, "A survey of privacy-enhancing technologies for IoT," *Ad Hoc Networks*, vol. 103, pp. 102–116 2020.
- [26] A. Rey, B. C. Chifor, and I. Bica, "Formal methods for IoT security: A survey," *Computers & Security*, vol. 97, pp. 101–133 2020.
- [27] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616-644, 2019.
- [28] M. Alam, J. Rufino, J. Ferreira, S. H. Ahmed, N. Shah, and Y. Chen, "Orchestration of microservices for IoT using Docker and edge computing," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 118–123, 2018.
- [29] P. Porambage, A. Braeken, A. Gurtov, and M. Ylianttila, "Secure lightweight authentication for resource-constrained IoT: A survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1709–1743, 2021.
- [30] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic mapping study (updated)," *IEEE Access*, vol. 8, pp. 213–246 2020.
- [31] M. S. Ferdous, F. Chowdhury, and Y. Aono, "A survey on authentication in IoT and CPS: Attacks, challenges, and open issues," *IEEE Access*, vol. 9, pp. 296–325, 2021.



- [32] A. Boudguiga, L. Granboulan, and R. Géraud, "Privacy-preserving authentication for connected objects using zero-knowledge proofs," *Computer Communications*, vol. 179, pp. 69–82, 2021.
- [33] G. Arfaoui, Y. Challal, and A. Bouabdallah, "Key agreement and authentication protocols in IoT: Taxonomy and performance evaluation," *Internet Things*, vol. 13, p. 100351, 2021.