Dandao Xuebao/Journal of Ballistics
ISSN: 1004-499X
Vol. 37 No. 1 (2025)

Tokenized Zero Trust Architecture for Social Internet of Things (SIoT): A Comprehensive Review

[1]Meena Rani, [2]Dr. Padathala Visweswara Rao, [3]Nairanjana Sarkar, [4]Ranjan Banerjee, [5]Raghavi S, [6]Shamim Ahmad khan

[1]Assistant Professor, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India, meena.rani@chitkara.edu.in

[2]associate Professor, Vignan's Institute of Information Technology, Duvvada sivaji1259@gmail.com

[3]Brainware University, nas.cs@brainwareuniversity.ac.in

[4]Brainware University, rnb.cse@brainwareuniversity.ac.in

[5]Assistant Professor, department of computer science and engineering, St. Joseph's college of Engineering, Chennai, raghavi.S.Selva@gmail.com

[6]Research scholar, Department of Electronics & Communication Engineering , Glocal school of science & technology. Glocal University , skwarsi@hotmail.com

Abstract: The Social Internet of Things (SIoT) has emerged as a powerful paradigm that enables smart devices not only to connect and communicate but also to build social relationships autonomously. While SIoT enhances usability, personalization, and intelligent services, it simultaneously introduces serious security and privacy concerns. This review explores the application of Tokenized Zero Trust Architecture (ZTA) as a comprehensive security model for SIoT ecosystems. By combining token-based identity management with the Zero Trust principle of "never trust, always verify," Tokenized ZTA provides an innovative framework for minimizing unauthorized access and insider threats in socially connected IoT environments. The paper critically analyzes current SIoT security frameworks, explores tokenization technologies (OAuth2, JWT, blockchain tokens), and examines Zero Trust implementation strategies tailored for decentralized, heterogeneous networks. Challenges such as scalability, interoperability, and computational overhead are discussed, alongside future directions for achieving dynamic, self-adaptive trust management in SIoT. The review also investigates cross-layer security implications, collaborative authentication frameworks, and the socio-technical impact of trust decentralization. This review aims to provide a foundational reference for researchers and developers seeking to build secure, scalable, and privacy-preserving SIoT systems.

Keywords: Social Internet of Things (SIoT), Zero Trust Architecture (ZTA), Tokenization, IoT Security, Identity Management, Privacy, Access Control, Blockchain, Decentralized Systems, Trust Management, Edge Computing

1. Introduction The Internet of Things (IoT) is evolving rapidly with the emergence of the Social Internet of Things (SIoT), a model where smart objects form social relationships mimicking human social networks. SIoT aims to enhance system intelligence, contextual awareness, and interoperability. As devices increasingly interact without direct human control, trust between autonomous entities becomes a critical concern. However, with these advancements come new vulnerabilities due to open, dynamic, and heterogeneous environments. Traditional perimeter-based security models fail to provide adequate protection in such distributed networks. This has led to the exploration of Zero Trust Architecture (ZTA), which enforces strict access control, continuous verification, and identity-centric authentication.

2. Fundamentals of SIoT and Security Challenges

- **Definition and Characteristics of SIoT:** The Social Internet of Things (SIoT) represents an extension of the traditional Internet of Things, where smart objects are not just interconnected but socially aware. In SIoT, devices can establish and manage social relationships based on contextual factors such as shared ownership, spatial proximity, functionality, and usage patterns. These relationships are categorized similarly to human social connections, including parental (same manufacturer), co-work (collaborative devices), co-location (devices in the same environment), and ownership (same user). The goal of SIoT is to improve service discovery, enhance contextual awareness, and enable devices to autonomously interact in a more meaningful,

intelligent way. Unlike classical IoT systems, SIoT nodes are designed with social behavior models that enable trust-building, recommendation generation, and dynamic network topology adaptation. These characteristics allow SIoT to support applications in smart homes, smart cities, healthcare, and industrial systems,fostering a new era of interaction between humans and intelligent devices.

- **Social Relationships Among Things:** In the Social Internet of Things (SIoT), smart devices are capable of forming autonomous social relationships with other devices to enhance collaboration, interoperability, and service delivery. These relationships are modeled after human social ties and categorized into various types, such as parental (devices from the same manufacturer or family), co-location (devices operating in the same physical environment), co-work (devices that collaborate to complete shared tasks), and ownership (devices belonging to the same user or household). Additionally, temporary relationships may be established for specific, short-term purposes, such as during device pairing in a public environment. These social bonds enable devices to build trust, recommend other reliable devices, and dynamically adapt to changing network conditions. The social relationship model is a fundamental pillar of SIoT, as it allows devices to filter interactions, prioritize connections, and form self-organizing networks that improve scalability, reliability, and contextual awareness in smart environments.
- **Key Security and Privacy Concerns in SIoT:** The Social Internet of Things introduces unique security and privacy challenges due to its dynamic, decentralized, and highly interconnected nature. In SIoT environments, devices interact autonomously and exchange sensitive data, making them vulnerable to a variety of attacks. Key concerns include identity spoofing, where malicious entities impersonate trusted devices; man-in-the-middle attacks, which intercept and alter communications; and unauthorized access, allowing intruders to manipulate or misuse device functionalities. Data privacy is a critical issue as personal and contextual information shared among devices can be exposed, leading to surveillance or profiling. Furthermore, the fluid social relationships among devices increase the difficulty of implementing consistent access controls and trust mechanisms. The lack of standardized security protocols across heterogeneous devices and platforms further compounds the risk, creating potential entry points for cyber threats. These challenges necessitate advanced, adaptive security architectures such as Zero Trust, capable of enforcing granular access policies and real-time verification in the SIoT ecosystem.
- **Limitations of Traditional Security Models in SIoT:** Traditional security models, which typically rely on perimeter-based defenses and static access control mechanisms, are ill-suited for the dynamic and decentralized architecture of the Social Internet of Things. These conventional frameworks assume predefined trust boundaries and centralized authorities, making them ineffective in SIoT environments where devices continuously join, leave, and interact in unpredictable patterns. The lack of persistent connectivity and uniform device capabilities in SIoT further complicates the implementation of consistent security policies. Additionally, centralized authentication systems can become single points of failure and bottlenecks for scalability. The static nature of traditional models fails to accommodate real-time context-aware decision-making required in SIoT scenarios. As a result, they are vulnerable to identity spoofing, unauthorized access, and data manipulation, especially when devices interact autonomously. These limitations necessitate a shift towards more flexible and adaptive security architectures like Zero Trust, which emphasize continuous verification, decentralized trust, and dynamic access control.

3. Zero Trust Architecture: Concepts and Components

Zero Trust Architecture (ZTA) is a cybersecurity model that operates on the principle of "never trust, always verify." Unlike traditional models that implicitly trust users or devices within a defined network perimeter, ZTA assumes that threats can come from both external and internal sources. This model requires strict identity verification for every person and device attempting to access resources on a network, regardless of their location. The core components of ZTA include the Policy Engine, which evaluates access requests based on identity, context, and policies; the Policy Administrator, which executes access decisions; and the Policy Enforcement Point, which ensures only authenticated and authorized access to resources. ZTA also relies on robust Identity and Access Management (IAM), multifactor authentication (MFA), micro-segmentation, and continuous monitoring to maintain security. In the context of SIoT, ZTA can dynamically adapt to changing

device behaviors and interaction contexts, making it well-suited for managing trust in highly distributed and autonomous networks. By shifting the focus from network perimeter to identity and context, ZTA offers a more resilient and granular approach to security for next-generation IoT systems.

4. Tokenization in Access Control

Tokenization in access control is a security technique that involves substituting sensitive authentication credentials with unique, non-sensitive tokens that can be safely used to verify identity and authorize access. In the SIoT context, tokenization serves as a foundational mechanism for enforcing decentralized and dynamic access policies. These tokens—such as JSON Web Tokens (JWTs), OAuth2 tokens, or blockchain-based identity tokens—carry encrypted metadata about user identity, device credentials, and access permissions. This approach significantly reduces the risk of credential theft and limits the impact of breaches, as tokens are designed for one-time or context-specific use. Tokenization also supports stateless authentication, enabling scalable and efficient access control in resource-constrained SIoT environments. Furthermore, it facilitates fine-grained access decisions based on real-time context, such as device behavior, location, and interaction history. By integrating token-based systems with Zero Trust principles, SIoT networks can achieve robust, adaptive security that aligns with the needs of highly mobile and autonomous device ecosystems.

5. Tokenized Zero Trust for SIoT

- **Integrating Tokenization with ZTA in SIoT:** Combines Zero Trust principles with token-based authentication and access control to dynamically assess trustworthiness of devices and interactions.
- **Use Case: Token-Based Access in Smart Home SIoT Network:** Devices request access tokens through a local gateway which verifies identity using blockchain. Access is granted based on policy, behavior, and contextual information.
- **Enhancing Trust Through Decentralized Identity Verification:** Devices establish trust autonomously through verifiable credentials and past interactions recorded on a distributed ledger.
- **Real-Time Authentication and Authorization Workflows:** Use of lightweight protocols (e.g., CoAP with DTLS, MQTT with TLS) ensures low latency, secure transactions across diverse SIoT environments.

6. Benefits and Limitations

- **Enhanced Security and Fine-Grained Access Control:** Every device is continuously authenticated, minimizing risks from compromised nodes.
- **Improved Scalability and Decentralization:** Tokenized ZTA supports growth without centralized bottlenecks.
- **Challenges:**
  - **Token Management Overhead:** Particularly in constrained devices.
  - **Computational Costs:** Especially in blockchain and encrypted token verification.
  - **Token Expiry and Synchronization:** Synchronizing token lifetimes across distributed systems can be complex.
  - **Revocation Complexity:** Securely revoking tokens without central coordination remains a challenge.

7. Future Directions and Research Opportunities

- **AI-Driven Dynamic Trust Evaluation Models:** Real-time trust score updates based on behavior, context, and feedback.
- **Lightweight Token Protocols for Resource-Constrained Devices:** Development of energy-efficient cryptographic schemes.
- **Interoperability Standards for Cross-Platform SIoT Trust:** Standard APIs and metadata models for token exchange.

- **Privacy-Preserving Token Generation and Usage:** Use of zero-knowledge proofs and homomorphic encryption.
- **Cross-Layer Security Integration:** Coordination across application, network, and transport layers to ensure cohesive security.
- **Collaborative Authentication Frameworks:** Multi-device consensus on identity and behavior for access validation.

8. Conclusion Tokenized Zero Trust Architecture represents a promising direction for securing the future of the Social Internet of Things. By leveraging identity-centric, continuous verification mechanisms and robust tokenization methods, ZTA addresses the core vulnerabilities of SIoT networks. As SIoT expands across homes, healthcare, transportation, and industry, security architectures must evolve to be both adaptive and scalable. This review synthesizes current developments and highlights critical research gaps, laying a foundation for designing next-generation secure SIoT systems that are resilient, privacy-aware, and intelligent.

References

[1] Bertino, E., & Islam, N. (2021). Security for the Internet of Things: A Survey. *ACM Computing Surveys*, 54(6), 1-37.
[2] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication 800-207*.
[3] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146-164.
[4] Wang, W., et al. (2019). Blockchain-Based Token Authentication for Secure Smart Home SIoT Networks. *IEEE Internet of Things Journal*, 6(5), 8463-8475.
[5] Qin, Y., et al. (2022). A Survey on Tokenization Techniques in Cybersecurity. *IEEE Access*, 10, 54012-54035.
[6] Rahman, M. A., Islam, M. R., & Hussain, F. K. (2020). Trust management in social Internet of Things: A review. *IEEE Internet of Things Journal*, 7(3), 2501-2515.
[7] Li, F., & Liu, J. (2021). A Review of Zero Trust Security Architectures in IoT. *Sensors*, 21(16), 5523.
[8] Zhang, K., et al. (2020). Edge intelligence and trust in smart IoT: From mechanism to applications. *IEEE Network*, 34(6), 66-73.