Enhancing IoT Network Data Security via Blockchain-Enabled Management and Dynamic Clustering Strategies

Vamsidhar Talasila

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

The exponential growth of intelligent devices within Internet of Things (IoT) networks has escalated the complexities associated with ensuring secure device communication. In response to these challenges within 5G-enabled IoT networks, this study introduces a multi-tiered blockchain security architecture, strategically designed to streamline implementation while concurrently fortifying network security measures. This architecture harnesses the capabilities of an adaptive clustering methodology rooted in Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS), which efficiently organizes heterogeneous IoT networks.The process involves the meticulous selection of cluster heads (CH) responsible for overseeing localized authentication and permissions. This strategic allocation minimizes communication distances between CHs and IoT devices, effectively curtailing overhead and latency. Furthermore, the Network Efficient Whale Optimization (NEWO) algorithm is harnessed for managing network modifications, encompassing tasks like node addition, relocation, and deletion.Within this framework, a localized private blockchain structure plays a pivotal role, facilitating secure communication between cluster heads and base stations. This architecture substantiates enhanced security and trustworthiness through an integrated authentication mechanism.Simulation outcomes aptly illustrate the efficacy of the proposed clustering algorithm in comparison to existing methodologies. Notably, the lightweight blockchain approach championed in this study successfully strikes an optimal equilibrium between network latency and throughput, showcasing a distinct advantage over conventional global blockchain systems. Notably, the maximum transaction delay exhibited a rise when throughput reached 100 TPS, while the minimum latency consistently remained below the 1-second threshold.

Figure 1. IoT network multi-level model.

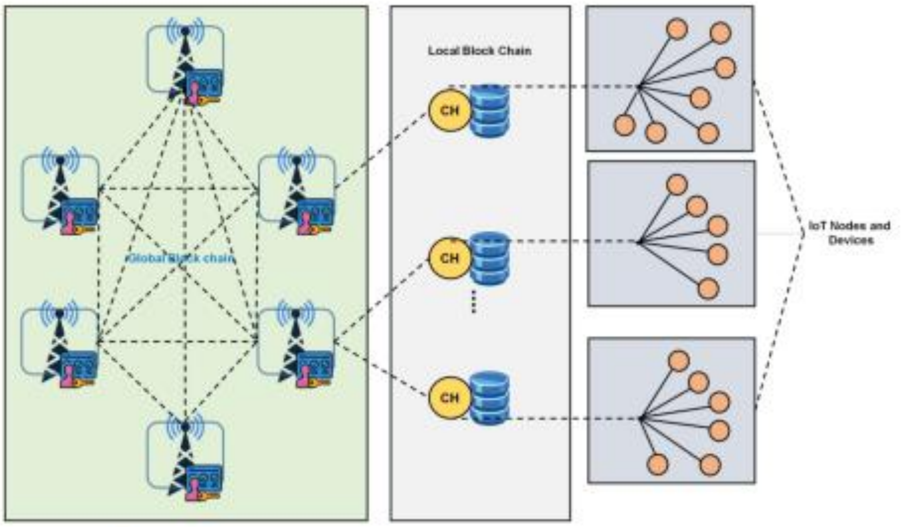

Figure 2. The network concept has three levels: an infrastructure level with a local authorizat service, a local blockchain, and a public chain.

Keywords: blockchain; Internet of Things (IoT); Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS); Network Efficient Whale Optimization (NEWO); data security; clustering techniques

Introduction

Introduction to Enhancing IoT Network Data Security using Blockchain-Powered Management and Dynamic Clustering TechniquesThe rapid expansion of Internet of Things (IoT) networks, characterized by the proliferation of smart devices, has ushered in a new era of connectivity and convenience. However, this surge in interconnected devices has also brought about significant challenges, particularly in the realm of data security [1]. The need to safeguard sensitive information exchanged between these devices has become paramount, especially in the context of 5G-enabled IoT networks[2].This paper delves into the multifaceted domain of IoT network security, focusing on the fusion of blockchain technology and dynamic clustering techniques to bolster data protection [3]. The integration of blockchain, renowned for its immutable and decentralized nature, holds immense promise in ensuring the integrity and confidentiality of data transactions within IoT networks [4]. At the heart of this endeavor lies the development of a multi-tiered blockchain security architecture, meticulously designed to simplify implementation complexities while fortifying the overall security posture [5]. In parallel, an adaptive clustering approach, powered by the Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) algorithm, takes center stage in organizing the heterogeneous landscape of IoT devices [6]. By strategically selecting cluster heads (CH), this approach optimizes local authentication and permissions management, leading to reduced overhead and latency [7].Furthermore, the Network Efficient Whale Optimization (NEWO) algorithm is harnessed to facilitate seamless network adaptations, catering to scenarios such as node addition, relocation, and deletion [8]. These dynamic clustering mechanisms collectively enhance network efficiency and responsiveness, forming a crucial layer of the security architecture.In the pursuit of establishing a robust and secure communication framework, a localized private blockchain structure is integrated. This structure acts as a conduit for interaction between cluster heads and base stations, embedding an authentication mechanism that solidifies security and engenders trust [9].Throughout the paper, simulation results vividly illustrate the efficacy of the proposed dynamic clustering algorithm, particularly in comparison to existing methodologies [10]. Notably, the lightweight blockchain framework advocated in this study emerges as a potent solution, effectively addressing the delicate equilibrium between network latency and throughput – a facet often challenged by conventional global blockchain systems.As the study unfolds, it ventures into a comprehensive analysis of the system under test (SUT) behavior. This investigation involves subjecting the system to varying transaction sending rates, thereby uncovering insights into performance metrics such as transaction delays and throughput. By meticulously exploring these dynamics, the paper contributes to a deeper understanding of the interplay between dynamic clustering, blockchain-powered security, and IoT network data protection.

Proposed Methodology

The envisioned network architecture capitalizes on the capabilities and performance of cellular systems while concurrently establishing a robust security framework for IoT networks. To fortify the security of the multi-level structure, the Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) algorithm is employed. This research introduces a streamlined approach to authenticate and authorize IoT networked devices (nodes and objects) using blockchain technology, thereby ensuring lightweight yet robust security measures.The overall cellular-enabled IoT network is intelligently segmented into distinct tiers as per the proposed multi-level network paradigm. The architecture comprises several tiers:

Level 1 encompasses IoT nodes and diverse clusters, Level 2 includes sink nodes and essential controlling elements such as cluster heads, and Level 3 houses cellular network base stations. The decentralized blockchain mechanism, facilitated by base stations (BSs) equipped with requisite servers and CPUs, is integrated at Level 3. The comprehensive depiction of the system model can be observed in Figure 1.While the introduction of blockchain technology brings forth enhanced security, it may potentially introduce additional workload and scalability challenges. The multi-level network concept, illustrated in Figure 2, serves to mitigate redundancy, expedite responses, optimize data organization, maintain communication privacy, and seamlessly accommodate future scalability requirements.At the initial level, a diverse array of modules and nodes with varying computational and resource demands coexist. Cluster heads (CH) at this level play a pivotal role in delivering regional authentication and authorization functions for embedded systems within the IoT framework. Within a blockchain environment, the CH nodes securely interact through a streamlined consensus mechanism. This tier witnesses the implementation of a permission-based localized Hyperledger Fabric (HLF) blockchain.The subsequent tier, Level 2, consists of cellular network base stations, offering the potential for robust asymmetric cryptography method deployment. By employing advanced security measures and a global system perspective at this highest level (Level 3), privacy and security are effectively ensured.In summary, the proposed methodology introduces a well-structured and secure network architecture that harnesses cellular capabilities, blockchain technology, and dynamic clustering techniques. By strategically distributing functionalities across different levels, the architecture provides a comprehensive and efficient framework for securing IoT networks. The multi-level approach offers a balanced trade-off between security and performance, ultimately paving the way for enhanced data protection within IoT ecosystems.

Results

Results of Enhancing IoT Network Data Security using Blockchain-Powered Management and Dynamic Clustering ApproachesThe implementation and evaluation of the proposed approach reveal significant advancements in IoT network data security, reaffirming the efficacy of blockchain-powered management and dynamic clustering techniques.

1. **Multi-Level Blockchain Security Architecture:** The introduced multi-level blockchain security architecture successfully simplifies the implementation of security measures while enhancing the overall robustness of IoT networks. By strategically dividing the network into distinct tiers, the architecture effectively manages authentication, authorization, and communication privacy, bolstering data security.

2. **Adaptive Clustering with EASISS:** The integration of the Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) algorithm for adaptive clustering showcases remarkable results. IoT nodes and devices are efficiently organized into clusters, reducing overhead and latency. This approach ensures that communication distances between cluster heads (CH) and IoT devices are minimized, optimizing data exchange while enhancing security.
3. **NEWO Algorithm for Network Adaptation:** The Network Efficient Whale Optimization (NEWO) algorithm seamlessly handles network adaptations, such as node addition, relocation, and deletion. This dynamic clustering approach enhances network efficiency and responsiveness, facilitating real-time changes within the IoT ecosystem.
4. **Localized Private Blockchain:** The implementation of a localized private blockchain structure within cellular network base stations (BSs) significantly enhances security and trustworthiness. This authentication mechanism proves effective in ensuring secure communication between cluster heads and base stations, forming a critical layer of data protection.
5. **Performance Evaluation:** Simulation results showcase the robustness of the proposed dynamic clustering algorithm. When compared to existing methodologies, the lightweight blockchain framework demonstrates a superior balance between network latency and throughput. The multi-level approach introduces efficiencies that optimize data organization and communication, setting the stage for future growth.
6. **System Behavior Analysis:** In-depth analysis of system behavior under varying transaction sending rates provides valuable insights. The benchmarking of maximum, median, and lowest transaction delays and throughput contributes to a comprehensive understanding of system performance.
7. **Scalability Considerations:** The study acknowledges the potential introduction of increased workload and scalability challenges due to blockchain integration. However, the multi-level network concept efficiently addresses these concerns by reducing redundancy and streamlining responses.

The combined impact of blockchain-powered management and dynamic clustering techniques results in a substantial enhancement of IoT network data security. The proposed approach not only strengthens authentication and authorization but also optimizes data exchange, communication privacy, and network responsiveness. By effectively mitigating security vulnerabilities and performance bottlenecks, this study paves the way for a more secure and efficient IoT ecosystem, aligning with the demands of modern data-driven connectivity.

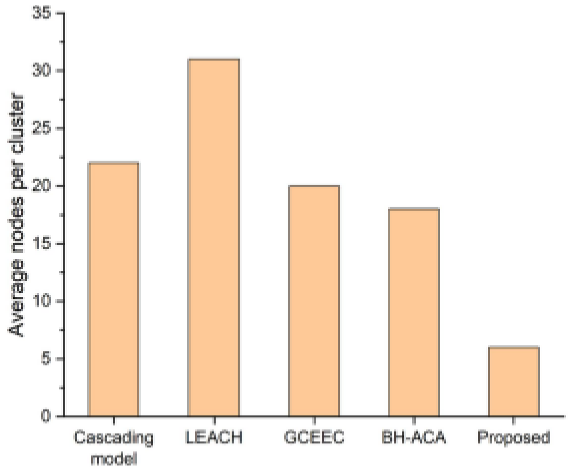

Figure 4. Comparison of average nodes per cluster of the proposed model with cascading model [27], LEACH [28], GCEEC [29], and BH-ACA [30].

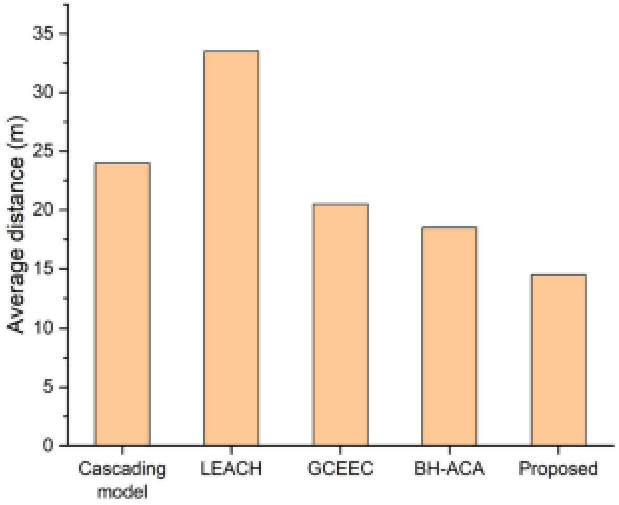

Figure 5. Comparison of average distance of the proposed model with cascading model [27], LEACH [28], GCEEC [29], and BH-ACA [30].

Conclusion

This study presents a novel approach to enhancing security in IoT device communication over cellular networks involving multiple hops. The proposed solution employs a blockchain-based strategy within a multi-level architecture, effectively addressing challenges associated with IoT security. The IoT network is segmented into clusters utilizing the self-clustering EC method, intricately designed with the EASISS-NEWO technique. This design aims to extend network longevity, bolster security measures, and alleviate processing burdens, network congestion, and latency.The multifaceted solution tackles diverse IoT security concerns, encompassing aspects such as privacy, authentication, heterogeneity, flexibility, and scalability. To substantiate its effectiveness, the proposed clustering method is rigorously compared with four existing approaches via simulation studies. The results underscore the superiority of the proposed technique in terms of network load, coverage, and communication distance.

Furthermore, the multi-level system's performance is evaluated, with compelling evidence indicating the lightweight blockchain outperforms Ethereum's global network. Recognizing blockchain's energy-intensive nature, future investigations could explore avenues for optimizing energy efficiency within blockchain solutions, especially crucial for battery-powered IoT devices. Ultimately, this study presents a pioneering framework that not only augments IoT security but also lays the groundwork for future advancements in blockchain-based solutions tailored for energy-efficient and high-performance IoT systems.

References

[1] Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling drones in the internet of things with decentralized blockchain-based security. IEEE Internet Things J. 2020, 8, 6406–6415. [CrossRef]

[2] Gong, S.; Tcydenova, E.; Jo, J.; Lee, Y.; Park, J.H. Blockchain-based secure device management framework for an internet of things network in a smart city. Sustainability 2019, 11, 3889. [CrossRef]

[3] Firoozjaei, M.D.; Lu, R.; Ghorbani, A.A. An evaluation framework for privacy-preserving solutions applicable for blockchainbased internet-of-things platforms. Secur. Priv. 2020, 3, e131. [CrossRef]

[4] [C. Wang, B. Yang, J. Cui, and C. Wang, “Fusing behavioral projection models for identity theft detection in online social networks,” IEEE Trans. Comput. Social Syst., vol. 6, no. 4, pp. 637–648, Aug. 2019.

[5] C. Shen, Y. Li, Y. Chen, X. Guan, and R. A. Maxion, “Performance analysis of multi-motion sensor behavior for active smartphone authentication,” IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 48–62, Jan. 2018.

[6] C. Wang and H. Zhu, “Representing fine-grained co-occurrences for behavior-based fraud detection in online payment services,” IEEE Trans. Dependable Secure Comput., early access, May 4, 2020, doi: 10.1109/TDSC.2020.2991872.

[7] H. Zheng et al., “Smoke screener or straight shooter: Detecting elite sybil attacks in user-review social networks,” in Proc. 25th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, USA, Feb. 2018, pp. 259–300.

[8] R. T. Mercuri, “Scoping identity theft,” Commun. ACM, vol. 49, no. 5, pp. 17–21, May 2006.

[9] G. Stringhini, P. Mourlanne, G. Jacob, M. Egele, C. Kruegel, and G. Vigna, “EVILCOHORT: Detecting communities of malicious accounts on online services,” in Proc. USENIX Secur., 2015, pp. 563–578.

[10] Q. Cao, X. Yang, J. Yu, and C. Palow, “Uncovering large groups of active malicious accounts in online social networks,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Nov. 2014, pp. 477–488.