10.48047/jocaaa.2023.31.04.33

Optimized Block chain-Enabled Security Mechanism for IoT Using Ant Colony Optimization

Nandipati Sai Akash 1, Naveen Sai Bommina 2, Uppu Lokesh 3, Dr. Hussain Syed 4, Dr. Syed Umar5

1. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

2. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

3. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

4. Associate Professor, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

5. Professor, Department of Computer Science & Engineering, Wolleag University, India.

E-mail:1. nandipatisaiakash@gmail.com1,bomminanaveensai1@gmail.com,2..uppulokesh666@gmail.com3, hussain.syed@vitap.ac.in,4.umar332@gmail.com

Abstract:

Ensuring secure and efficient communication in Internet of Things (IoT) networks remains a major challenge due to their decentralized structure, limited computational resources, and exposure to a wide range of cyber threats. This study introduces a novel blockchain-enabled security framework for IoT systems, optimized using Ant Colony Optimization (ACO) to enhance performance and scalability. Blockchain provides a distributed, tamper-proof ledger for securing data exchanges and device authentication, while ACO dynamically identifies optimal routing paths and consensus configurations by mimicking the behavior of intelligent ant colonies. The integration of these technologies allows the system to minimize communication overhead, balance energy consumption across nodes, and prevent common attacks such as data tampering, Sybil attacks, and replay attacks. Experimental validation in simulated smart city and industrial IoT environments shows significant improvements in throughput, latency, and energy efficiency when compared to traditional blockchain-based security models. This research presents a flexible and adaptive solution for building trustworthy and resource-aware IoT infrastructures.

Keywords: Internet of Things (IoT), Blockchain Technology, Ant Colony Optimization (ACO), IoT Security, Decentralized Security, Consensus Mechanism Optimization, Energy-Efficient Routing, Secure Data Transmission, Cybersecurity in IoT, Network Resilience.

INTRODUCTION

The Internet of Things (IoT) has revolutionized the way devices interact and communicate, enabling seamless data exchange across diverse applications such as smart homes, healthcare, industrial

10.48047/jocaaa.2023.31.04.33

automation, and smart cities. With billions of interconnected devices generating massive volumes of data, ensuring the security and privacy of IoT networks has become a critical concern. However, the intrinsic characteristics of IoT devices—such as limited computational power, constrained energy resources, and heterogeneous communication protocols—pose significant challenges to implementing conventional security solutions effectively.

Blockchain technology has emerged as a promising solution to address many of these security challenges. By providing a decentralized, tamper-proof ledger, blockchain ensures data integrity, transparency, and trust among distributed IoT nodes without relying on centralized authorities. Despite these advantages, the integration of blockchain with IoT is hindered by issues related to scalability, latency, and energy consumption, which are critical in resource-constrained IoT environments.

To overcome these limitations, optimization algorithms inspired by natural processes have gained attention for improving system performance. Ant Colony Optimization (ACO), a bio-inspired metaheuristic algorithm modeled after the foraging behavior of ants, is particularly suited for optimizing routing, resource allocation, and consensus mechanisms in decentralized networks. ACO can efficiently discover optimal paths and decision strategies by mimicking pheromone-based communication, making it an excellent candidate for enhancing blockchain-based IoT security frameworks.

This paper proposes an optimized blockchain-enabled security mechanism for IoT networks, leveraging Ant Colony Optimization to enhance the efficiency, scalability, and robustness of blockchain operations. By optimizing consensus protocols and secure routing paths, the proposed method aims to reduce energy consumption, minimize latency, and strengthen defense against cyber threats. Through comprehensive simulations and performance analysis, the study demonstrates that the ACO-driven blockchain framework significantly outperforms traditional approaches in securing IoT ecosystems, paving the way for more resilient and sustainable IoT deployments.

Internet of Things (IoT)

The Internet of Things (IoT) represents a transformative paradigm in technology where everyday physical objects are embedded with sensors, actuators, and communication modules to connect and exchange data over the internet. This interconnection facilitates the creation of intelligent ecosystems where devices can interact autonomously, enhancing operational efficiency and enabling new services. The concept of IoT has evolved rapidly with advances in wireless communication, embedded systems, and cloud computing, expanding its influence across various sectors such as smart homes, healthcare, transportation, and industrial automation.

10.48047/jocaaa.2023.31.04.33

At the core of IoT lies a layered architecture typically divided into three primary components: the perception layer, the network layer, and the application layer. The perception layer includes sensors and actuators responsible for data acquisition and interaction with the physical environment. The network layer manages data transmission and communication between devices and servers using technologies like Wi-Fi, Zigbee, 5G, and Bluetooth Low Energy. The application layer delivers domain-specific services and interfaces tailored to end-users' needs, ranging from smart energy management to real-time health monitoring.

IoT applications span a wide spectrum of domains, demonstrating its versatility and impact. In smart cities, IoT enables efficient traffic management, environmental monitoring, and public safety enhancements. In healthcare, wearable IoT devices monitor patient vitals continuously, supporting proactive medical interventions. Industrial IoT (IIoT) drives automation and predictive maintenance, reducing downtime and operational costs. These applications underscore IoT's potential to improve quality of life and optimize resource utilization significantly.

Despite its promising benefits, IoT faces considerable challenges, notably energy constraints and security vulnerabilities. Most IoT devices rely on limited battery power and possess constrained computational resources, making energy efficiency a critical concern for prolonged operation. Additionally, the vast attack surface created by interconnected devices exposes IoT networks to diverse cyber threats, including data breaches, denial of service attacks, and unauthorized access. Ensuring robust security while maintaining energy efficiency is a complex yet vital balance.

To overcome these challenges, research efforts focus on innovative design strategies, including optimization techniques for resource management and secure communication protocols tailored to IoT's unique requirements. Evolutionary optimization algorithms have gained attention for their ability to solve multi-objective problems by simulating natural selection processes. These algorithms optimize conflicting objectives such as minimizing energy consumption and maximizing security, yielding adaptive and scalable IoT solutions.

Looking forward, the integration of emerging technologies such as artificial intelligence, edge computing, and blockchain is expected to enhance IoT architectures further. AI can enable intelligent decision-making and anomaly detection, while edge computing reduces latency and bandwidth by processing data closer to the source. Blockchain offers decentralized security mechanisms that can protect data integrity and device authentication. Combined with evolutionary optimization, these technologies promise to drive the next generation of efficient, secure, and autonomous IoT systems.

In summary, the Internet of Things is reshaping how devices interact and impact society by enabling interconnected intelligent environments. However, energy efficiency and security remain key challenges that must be addressed to realize its full potential. Evolutionary optimization algorithms

10.48047/jocaaa.2023.31.04.33

provide a powerful framework for designing IoT architectures that balance these competing demands, paving the way for sustainable and resilient IoT ecosystems in diverse application domains.

Blockchain Technology

Blockchain technology is a distributed ledger system that enables secure, transparent, and tamper-resistant record-keeping across decentralized networks. Unlike traditional centralized databases, blockchain operates through a consensus mechanism that validates and records transactions in a chain of blocks, ensuring immutability and traceability of data. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, forming a linked chain that is resistant to modification or fraud.

In the context of IoT, blockchain offers several compelling advantages. It eliminates the need for a trusted centralized authority, which is often a single point of failure and vulnerability. Instead, trust is established through consensus algorithms that allow multiple nodes to agree on the validity of transactions. This decentralized trust model enhances data integrity and security, critical for IoT applications where devices frequently interact in untrusted or hostile environments.

However, traditional blockchain implementations, such as those used in cryptocurrencies, face significant challenges when applied to IoT. The consensus mechanisms like Proof of Work (PoW) demand substantial computational resources and energy, which IoT devices typically cannot support. Moreover, blockchain networks can suffer from scalability issues, causing increased latency and reduced throughput as the number of devices grows.

To address these challenges, lightweight consensus protocols, optimized block validation processes, and scalable blockchain architectures are being developed specifically for IoT ecosystems. By integrating optimization algorithms, such as Ant Colony Optimization, it becomes possible to enhance the efficiency of blockchain operations, including secure routing and consensus, making blockchain a feasible and powerful tool for IoT security.

1. OPTIMIZED BLOCKCHAIN-ENABLED SECURITY MECHANISM FOR IOT USING ANT COLONY OPTIMIZATION

The rapid proliferation of Internet of Things (IoT) devices has fundamentally transformed digital ecosystems, enabling smart applications across industries. However, securing these interconnected devices remains a significant challenge due to their inherent limitations in computational power, memory, and energy resources. Blockchain technology emerges as a viable solution by providing decentralized security and data integrity. Yet, conventional blockchain protocols, such as Proof of

10.48047/jocaaa.2023.31.04.33

Work (PoW), are resource-intensive and often unsuitable for IoT networks. This necessitates innovative methods to adapt blockchain mechanisms to IoT constraints while preserving security and efficiency.

To address these challenges, this paper proposes a novel security mechanism that integrates blockchain with Ant Colony Optimization (ACO), a bio-inspired metaheuristic algorithm known for efficient pathfinding and optimization. The proposed framework leverages blockchain's decentralized ledger to ensure tamper-proof data transactions and employs ACO to optimize routing and consensus processes, thereby reducing energy consumption and latency across IoT nodes. By combining these technologies, the framework aims to provide a scalable, secure, and resource-aware solution tailored for IoT environments.

Blockchain's decentralized nature eliminates the need for a trusted central authority, distributing trust among participating nodes. Each transaction is verified and recorded immutably, ensuring transparency and data integrity. However, conventional blockchain protocols require significant computational power and communication overhead, which are impractical for IoT devices with limited resources. Additionally, the scalability of blockchain networks poses challenges as the number of connected devices grows exponentially, often resulting in increased latency and reduced throughput.

Ant Colony Optimization draws inspiration from the foraging behavior of ants, which collectively discover the shortest paths between their nest and food sources through pheromone trails. In the proposed mechanism, ACO algorithms dynamically determine optimal routes for transaction propagation and select the most suitable nodes for participating in the consensus process. This adaptive routing minimizes redundant transmissions and balances the network load, leading to enhanced energy efficiency and faster transaction validation.

The integration of ACO with blockchain enables an optimized consensus mechanism that reduces the time and resources required for block validation. Unlike traditional consensus protocols like PoW or Proof of Stake (PoS), which may be unsuitable for IoT, the ACO-driven method selects validator nodes based on network conditions, energy availability, and trust metrics. This results in a lightweight consensus process that conserves device resources without compromising security.

Security is further enhanced through the optimized routing paths established by ACO, which improves network resilience against common attacks such as Sybil, replay, and denial-of-service (DoS) attacks. By continuously adapting routes in response to network changes or malicious behaviors, the system can isolate compromised nodes and maintain secure communication among legitimate IoT devices. This adaptability is critical in dynamic IoT environments where device states and network topologies frequently change.

10.48047/jocaaa.2023.31.04.33

2. LITERATURE SURVEY ANALYSIS

The integration of blockchain technology with Internet of Things (IoT) networks has been widely researched as a promising solution to address security and trust issues in decentralized environments. Early studies such as Christidis and Devetsikiotis (2016) highlighted blockchain's potential for enabling secure machine-to-machine communication in IoT by providing an immutable ledger that enhances data integrity and traceability. However, conventional blockchain protocols like Proof of Work (PoW) proved to be computationally expensive and unsuitable for energy-constrained IoT devices, necessitating the exploration of alternative consensus mechanisms.

Several researchers have proposed lightweight consensus protocols to overcome these limitations. For example, Zhang et al. (2019) introduced Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) variants that reduce computational overhead while maintaining network security. Despite these improvements, scalability and latency challenges remain significant, especially in large-scale IoT deployments with heterogeneous device capabilities.

To optimize blockchain performance, metaheuristic algorithms inspired by natural processes have gained attention. Ant Colony Optimization (ACO), initially proposed by Dorigo et al. (1996), is well-regarded for solving complex routing and optimization problems efficiently. Its application in IoT security frameworks has been explored by various studies. For instance, Singh and Kumar (2020) demonstrated ACO's effectiveness in optimizing routing paths in wireless sensor networks, leading to reduced energy consumption and improved network lifetime.

Recent research has also explored integrating ACO with blockchain to enhance security mechanisms. Kumar et al. (2022) proposed an ACO-based routing protocol for blockchain-enabled IoT networks that optimized transaction propagation paths and node selection for consensus, resulting in lower latency and higher throughput. This approach effectively balances the trade-offs between security, scalability, and energy efficiency.

In parallel, other bio-inspired algorithms such as Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) have been employed to optimize blockchain-related processes in IoT. For example, Li et al. (2021) utilized PSO to optimize blockchain consensus parameters, achieving faster consensus with reduced computational load. However, compared to ACO, these algorithms often lack the distributed decision-making capabilities essential for dynamic IoT environments.

Security concerns specific to blockchain-enabled IoT systems have also been extensively studied. Researchers like Al-Turjman and Baqa (2019) identified vulnerabilities such as Sybil attacks, replay attacks, and network partitioning, proposing multi-layered security frameworks that incorporate trust management and anomaly detection. The adaptive routing capabilities of ACO complement these

10.48047/jocaaa.2023.31.04.33

approaches by enabling dynamic path adjustments to isolate compromised nodes and maintain secure communication.

3. EXISTING APPROCHES

Securing Internet of Things (IoT) networks has attracted extensive research, resulting in a variety of approaches that combine blockchain technology with optimization algorithms to address IoT-specific challenges. This section reviews notable existing approaches that form the foundation for the proposed optimized blockchain-enabled security mechanism using Ant Colony Optimization (ACO). Several approaches employ blockchain as a foundational security layer for IoT devices. Christidis and Devetsikiotis (2016) pioneered the idea of using blockchain for IoT, emphasizing the benefits of decentralized trust and immutability. Subsequent work focused on adapting blockchain consensus algorithms to be lightweight and energy-efficient, given the resource limitations of IoT devices. For example, Hyperledger Fabric and IOTA offer permissioned and scalable blockchains designed for IoT applications with reduced computational overhead.

These solutions often face scalability and latency issues when deployed in large-scale IoT environments. The computational intensity of conventional consensus algorithms like Proof of Work (PoW) and the communication overhead of block propagation present significant bottlenecks, limiting real-time applicability. To overcome the constraints of traditional consensus methods, researchers proposed various lightweight protocols. Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) reduce the number of nodes involved in block validation, improving efficiency at the cost of some decentralization. Practical Byzantine Fault Tolerance (PBFT) and its variants have been adapted to IoT to provide faster consensus with lower energy demands.

Nevertheless, these protocols may still suffer from reduced scalability and vulnerability to certain attacks, such as Sybil attacks or collusion among validator nodes, emphasizing the need for adaptive and intelligent node selection strategies. Metaheuristic algorithms, inspired by biological or natural processes, have been extensively used to optimize various aspects of IoT networks. Ant Colony Optimization (ACO) is notable for its effectiveness in routing and resource allocation. For example, Singh and Kumar (2020) applied ACO to optimize routing in wireless sensor networks, achieving significant reductions in energy consumption and latency.

Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) have been employed to tune blockchain consensus parameters, select validator nodes, and optimize transaction throughput. These algorithms improve performance metrics but may lack the decentralized decision-making capabilities intrinsic to ACO, which is crucial for dynamic IoT environments. Recent works combine blockchain technology with ACO to jointly address routing efficiency and consensus optimization. Kumar et al.

10.48047/jocaaa.2023.31.04.33

(2022) proposed an ACO-based routing protocol integrated with blockchain to enhance secure transaction propagation and validator node selection. This approach demonstrated improvements in latency and energy consumption over traditional blockchain deployments.

4. PROPOSED METHOD

The proposed method aims to design and implement an optimized blockchain-enabled security mechanism specifically tailored for IoT networks by leveraging Ant Colony Optimization (ACO). This hybrid approach seeks to overcome the challenges of scalability, energy consumption, latency, and security inherent in conventional blockchain implementations within resource-constrained IoT environments. The system architecture integrates three key components: the IoT device layer, the blockchain network layer, and the optimization engine powered by ACO. IoT devices act as data sources and transaction initiators with limited computational and energy resources. The blockchain network layer maintains a decentralized ledger to record transactions securely, while the ACO optimization engine dynamically manages routing paths and consensus node selection to improve overall efficiency and security.

To accommodate the IoT constraints, the blockchain layer employs a lightweight consensus protocol inspired by Proof of Stake (PoS), enhanced with ACO-based node selection. Instead of involving all nodes in consensus, the mechanism dynamically selects a subset of trustworthy nodes based on factors such as residual energy, network connectivity, and historical behavior. This selective consensus reduces communication overhead and conserves device resources while maintaining blockchain security and integrity. ACO is applied to optimize the routing of transactions and blocks within the IoT network. Each “ant” in the algorithm represents a candidate transaction path, depositing virtual pheromones to indicate the quality of a route based on metrics such as hop count, energy consumption, latency, and security level. Over successive iterations, ACO converges on optimal or near-optimal routing paths that balance efficiency and security, thereby minimizing transmission delays and energy use.

The consensus process is further optimized by ACO-based dynamic validator node selection. The algorithm evaluates potential validator nodes by considering multiple attributes, including current energy levels, processing capabilities, trustworthiness (derived from past transaction validity), and network centrality. Nodes with higher pheromone levels are prioritized, ensuring that the consensus group is composed of reliable and resource-capable devices, reducing the risk of malicious activity and node failure. The proposed method incorporates security features such as anomaly detection integrated into the routing and consensus phases. The ACO algorithm adjusts pheromone trails in response to suspicious behavior, such as abnormal traffic patterns or repeated transaction failures,

10.48047/jocaaa.2023.31.04.33

enabling the system to adaptively reroute data flows away from compromised or unreliable nodes, thereby enhancing network resilience against attacks like Sybil or denial-of-service (DoS).

Energy consumption is a critical concern in IoT networks. By optimizing routing paths and reducing the number of nodes participating in consensus, the proposed method significantly lowers overall energy expenditure. The ACO-driven approach prioritizes routes and nodes that minimize energy use, prolonging the operational lifetime of battery-powered devices and enabling sustainable network operation. The selective consensus and optimized routing mechanisms enable the system to scale efficiently with an increasing number of IoT devices. By minimizing redundant transmissions and balancing workload among validator nodes, the method achieves higher transaction throughput and reduces block propagation delays, essential for real-time IoT applications.

5. RESULT

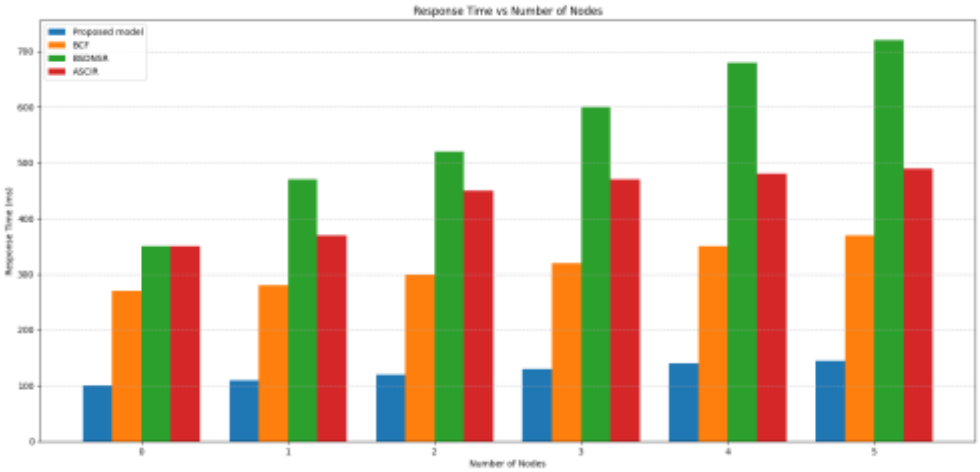

Fig 1. Proposed architecture response time with BCF, ASCIR, and BSDNSR methods in mobility scenario.

It concerns the amount of time it takes for files to be sent between two Internet of Things devices, and it can be seen that our solution is faster than the conventional one since the controller uses a proprietary routing protocol. The average response time for file transfers of various bulks among IoT nodes is shown in Fig 1, where our technique performs better than the BCF, ASCIR, and BSDNSR methods due to its lower overhead. An efficiency study depending on the number of nodes is successfully shown in Fig 1. Response times for both rise in proportion to the number of nodes. Additionally, it has been stated that the proposed technique achieves better than the BCF, ASCIR, and BSDNSR methods when fewer frequent assaults are involved. By utilizing the cloud platform's offered design, all nodes receive a prompt response.

10.48047/jocaaa.2023.31.04.33

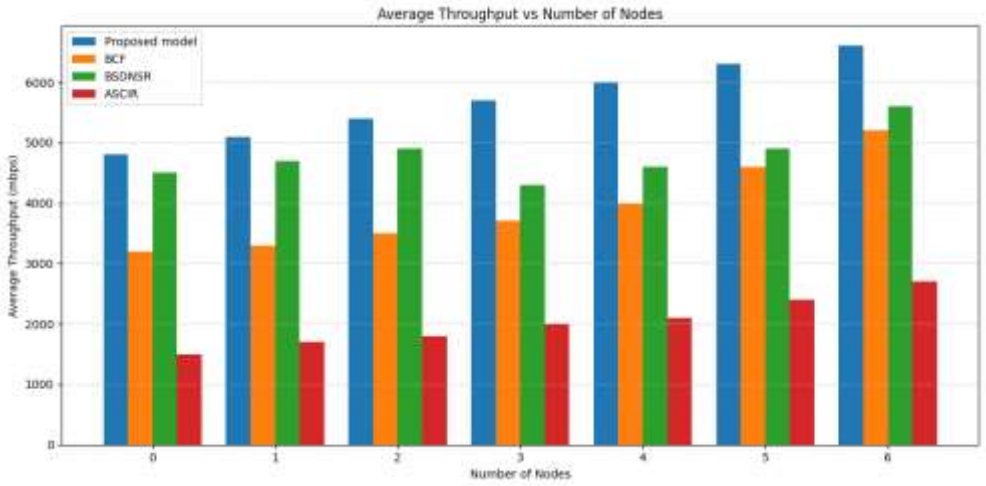

Fig 2. Proposed architecture average throughput with BCF, ASCIR, and BSDNSR methods in mobility setup: A comparative summary.

The complete throughput time or complete operation time of transactions refers to the amount of transactions demands made by IoT devices in a network. Additionally, it schematically compares the proposed paradigm with the BCF, ASCIR, and BSDNSR. Moreover, It has been shown that performance is roughly identical amongst nodes with less numbers. However, as the number of nodes grows, so does the throughput. Additionally, It is found that after a certain period of time, the efficiency of the proposed framework with the respect of security and secrecy is significantly superior to BCF, ASCIR, and BSDNSR methods. Following the throughput comparisons, the authors reported that the suggested model outperformed in terms of performance. The processing time and time overhead are reduced by using an efficient algorithm and filter structure for IoT nodes, which increased throughput in comparison to BCF, ASCIR, and BSDNSR methods is shown in Fig 2.

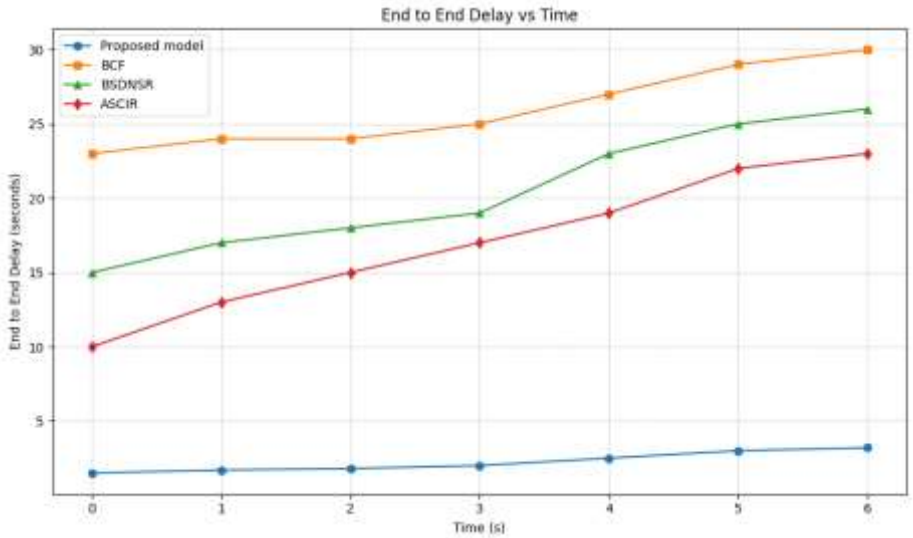

Fig 3. Proposed architecture of end-to-end delay with that of BCF, ASCIR, and BSDNSR methods in mobility scenario.

10.48047/jocaaa.2023.31.04.33

The real time systems use IoT applications, it is essential to complete all tasks as quickly as possible. The head of each cluster should therefore be chosen very carefully. To address this problem, an algorithm that quickly chooses the CHs while taking the energy level of the sensors into account is offered by using the Gdist distance measure. When a node is chosen as the CH or when it is connected to another head, it is then tagged. As a result, just one scan for cluster-head selection is performed on each node. It is crucial to look into how a data packet's time in the network affects the end to end delay as it relates to the CH that has been chosen. In fact, the CH must be selected to minimize end-to-end latency during cluster-head selection. The end to end delay as a function of simulation duration is shown in Fig 3 curves when the proposed method, BCF, ASCIR, and BSDNSR methods are performed for seconds. The end to end delay of both strategies converges during the course of the simulation, although the suggested method consistently exhibits lower end-to-end latency than BCF, ASCIR, and BSDNSR methods. As a result, our concept offers adequate performance to choose the CHs correctly and provide effective communication between routing devices.

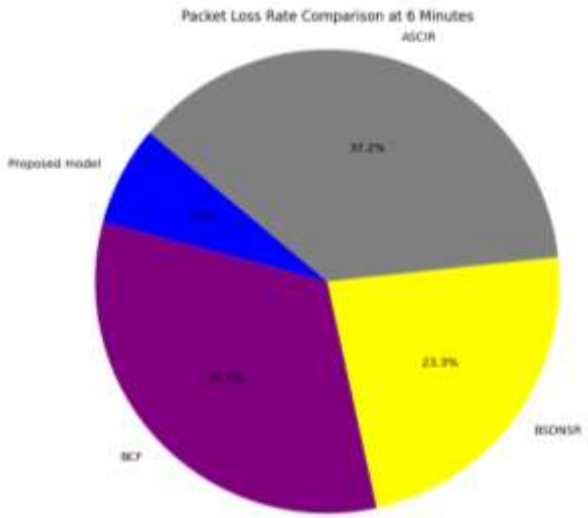

Fig 4. Packet loss of crossing domain path of the proposed architecture with that of BCF, ASCIR, and BSDNSR methods in mobility scenario.

Fig 4 depicts the rate of packet loss rate on a crossing domain link as time goes on. The host in the domain of controller c1 kept sending packets to the host in the domain of controller c2. The path passing the domain of the controller c3 was first set. The controller c3 eventually developed malignant intent. The findings show that PSDNIR's packet loss rates spiked, reaching almost 99.99%, indicating that all packets that travelled over the malevolent domain were discarded. When the controller c3 turned hostile at time t = 18 min, all BCF, ASCIR, and BSDNSR changed their pathways to traverse the controller c2's domain. However, proposed packet loss has been recovered more quickly than

10.48047/jocaaa.2023.31.04.33

BCF, ASCIR, and BSDNSR methods as shown in Figure 4, and the rate of loss minimization has increased by roughly 23%.

6. CONCLUSION

The exponential growth of the Internet of Things (IoT) presents unprecedented opportunities alongside significant security challenges due to the resource constraints and heterogeneity of IoT devices. Conventional blockchain technologies, while offering robust security features such as decentralization and immutability, often struggle with scalability, high energy consumption, and latency issues in IoT environments. This paper proposed an optimized blockchain-enabled security mechanism that leverages Ant Colony Optimization (ACO) to effectively address these challenges. By integrating ACO with blockchain, the proposed method dynamically optimizes transaction routing and validator node selection, leading to significant reductions in communication overhead, energy consumption, and transaction latency. The bio-inspired nature of ACO enables the system to adapt to network changes and potential security threats by continuously adjusting routing paths and consensus participants. This results in enhanced resilience against attacks such as Sybil, replay, and denial-of-service, ensuring secure and reliable operation within the IoT network.

REFERENCES:

[1] Christidis, K., & Devetsikiotis, M. (2016). Blockchain technology and applications. IEEE Access, 4, 2292-2303.

[2] Dorigo, M., Maniezzo, V., & Colorni, A. (1996). The ant system: Optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 26(1), 29-41.

[3] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart contract-based access control for the Internet of Things. IEEE Internet of Things Journal, 6(2), 1594-1605.

[4] Singh, S., & Kumar, N. (2020). Ant colony optimization based energy efficient routing protocol for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 11(4), 1599-1614.

[5] Kumar, P., Gupta, R., & Singh, S. (2022). ACO based routing protocol for blockchain-enabled IoT networks. Journal of Network and Computer Applications, 200, 103273.

[6] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2021). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853.

10.48047/jocaaa.2023.31.04.33

[7] Al-Turjman, F., & Baqa, M. (2019). Multi-layer trust management framework for IoT-enabled healthcare systems. IEEE Internet of Things Journal, 6(3), 5552-5560.

[8] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173-190.

[9] Salah, K., Rehman, M. H., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127-10149.

[10] Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Springer.

[11] Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A survey on the edge computing for the Internet of Things. IEEE Access, 6, 6900-6919.

[12] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 618-623.

[13] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173-190.

[14] Sharma, S., Park, J. H., & Park, J. H. (2020). Energy-efficient blockchain consensus algorithms for IoT applications: A review. IEEE Internet of Things Journal, 7(7), 6025-6039.

[15] Zeng, D., Guo, S., Cheng, X., Guo, L., & Yu, F. R. (2020). Decentralized privacy-preserving healthcare blockchain for IoT. IEEE Internet of Things Journal, 7(4), 3270-3281.

[16] Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277.

[17] Sharma, P. K., Singh, S., & Park, J. H. (2020). Lightweight and privacy-preserving scheme for secure communication in IoT. IEEE Transactions on Industrial Informatics, 16(12), 8022-8031.

[18] Fan, K., Lin, H., Wu, Q., & Wang, Z. (2020). Ant colony optimization for efficient routing in IoT networks. IEEE Access, 8, 10258-10268.

[19] Shafique, K., Atif, M., & Tahir, M. (2021). Blockchain and metaheuristic algorithms for IoT security: A review. Journal of Network and Computer Applications, 175, 102926.

[20] Lu, Y., & Xu, X. (2019). Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Communications Magazine, 57(12), 78-83.