International Journal of Safety and Security Engineering
Vol. 15, No. 12, December, 2025, pp. 2459-2469
Journal homepage: http://iieta.org/journals/ijsse

Performance Optimization in Blockchain-Based Approach to Secure Communication Channel in the Fifth Generation (5G) Authentication Mechanism

Nida Al-Shafi*, Nidal Turab

Department of Networks and Cybersecurity, Al-Ahliyya Amman University, Amman 19328, Jordan

Corresponding Author Email: n.shafi@ammanu.edu.jo

https://doi.org/10.18280/ijsse.151204

Received: 16 October 2025
Revised: 15 December 2025
Accepted: 23 December 2025
Available online: 31 December 2025

Keywords:
Authentication and Key Agreement, Blockchain, performance, throughput, latency, resource utilization, security, consortium Blockchain

ABSTRACT

Technological advancements in Fifth Generation (5G) technology have contributed to the emergence of enhanced network capabilities. In this context, network security is essential. Traditional authentication mechanisms encounter certain challenges, particularly the reliance on a secure link between the Serving Network (SN) and the Home Network (HN). Researchers proposed using Blockchain to secure 5G communication channels. However, their suggested methodologies have encountered several challenges related to network performance, which impact the applicability of their approaches. This paper proposes an innovative approach using a consortium Blockchain with a dynamic block size to enhance system performance while maintaining security. This paper presents empirical experiments comparing the dynamic block size approach with the fixed block size approach suggested by researchers (One transaction per block and 1 megabyte per block) under real traffic distribution. The experimental results showed that the dynamic block size approach yielded a success rate of 97.18% with an average latency of 1.29 seconds. In the one transaction per block scenario, the success rate was 26.97%, and the delay was 6.204 seconds. Finally, the 1MB approach had a success rate of 0%, a delay of 375.42 seconds. The proposed methodology offers a practical approach for protecting communication channels in 5G technology through Blockchain.

1. INTRODUCTION

The world is rapidly approaching the Fifth Generation (5G) era of telecommunication, where the way to communicate will change dramatically due to the incomparable features afforded by this technology in terms of high-speed connectivity, tremendous capacity, and negligible latency, in addition to superior user experience satisfaction. This opens the door widely to achieving the dream of ultra-reliable communication, i.e., smart cities, massive machine-to-machine communication, and the Internet of Things (IoT), in addition to enhancing mobile broadband capabilities [1].

5G deployment, on the other hand, introduced new security challenges and many more network security risks by having a wide attack surface where millions of devices will be connected to the network, and attackers can take advantage of IoT devices to attack the network by exploiting their hardware vulnerabilities [1, 2]. It is important to acknowledge that the occurrence of attacks and threats targeting 5G networks can result in significant financial losses. Consequently, safeguarding network security has become an imperative necessity that cannot be overlooked. Furthermore, individuals consider their personal data stored online to be confidential information, accessible only to authorized persons. Therefore, compromising or neglecting security measures is not an option [2, 3].

The Fifth Generation–Authentication and Key Agreement (5G-AKA) protocol is a security procedure used between the 5G core network and the User Equipment (UE) to authenticate and establish security keys. It can be considered the most crucial part of the overall 5G security architecture, which aims to provide end-to-end security for 5G communications. The current 5G-AKA protocol is standardized and defined in 3GPP TS 33.501, which establishes the technical requirements for 5G and other mobile telecommunications standards. The 3GPP security team reported numerous weaknesses in the authentication mechanism, encouraging researchers to develop countermeasures for these potential threats and propose their solutions. One of the key challenges is the assumption of having a secure channel between the Serving Network (SN) and the Home Network (HN) [4, 5].

The channel between the SN and the HN offers confidentiality, integrity, authenticity, and replay protection [TS 33.501, Sec. 5.9.3]. Figure 1 presents the threat model relevant to the 5G-AKA protocol, focusing on the communication channel. Active attackers can eavesdrop, manipulate, intercept, and inject messages in the channel between the subscribers and SNs. Where the passive attacker overhears signaling messages (i.e., messages transmitted on the physical layer). Then the attacker establishes a rogue base station which transmits and receives signaling messages, e.g., to mimic SNs [6].

In the basic threat model, active attack vectors can perform several attacks, such as Man-In-The-Middle (MITM) attacks. Authentication messages transferred between SN and HN can be modified or injected, enabling the creation of counterfeit responses or altering the data sent. In addition, the figure depicts a signaling-based Denial-of-Service (DoS) attack, in which excessive or malicious authentication requests overwhelm the SN-HN interface and may exhaust the computational and network resources used by the core authentication parties. Prior authors conducted a formal analysis and highlighted the need for stronger trust mechanisms. Specifically, it explains why the sole use of secure tunnels cannot be regarded as sufficient under cross-domain trust models, which highlights the need to deploy a distributed, verifiable, and tamper-resistant design, such as the Blockchain-based solution [6-8].

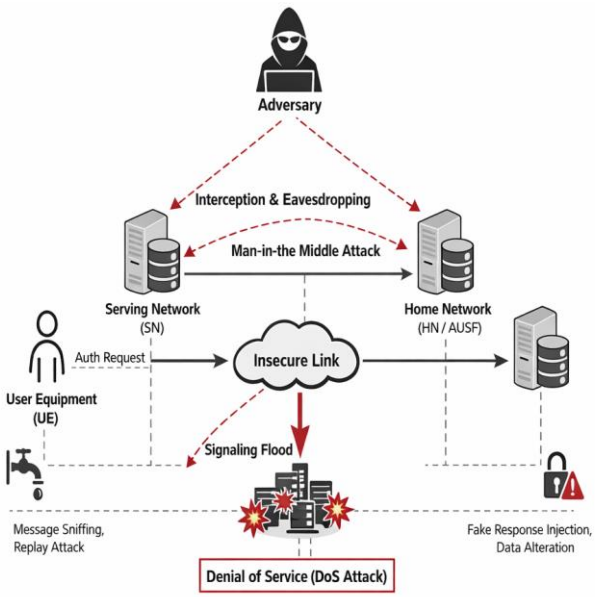

Figure 1. Threat model of the Fifth Generation–Authentication and Key Agreement (5G-AKA) protocol under weakened Serving Network–Home Network (SN-HN) secure channel assumptions

To address this issue, researchers in academia have proposed incorporating Blockchain technology due to its inherent security features make it a promising solution to combat DoS and Distributed Denial of Service (DDoS) attacks, as it is based on decentralized logic that eliminates a single point of failure [9-12].

To address this challenge, researchers have explored the use of Blockchain technology, which offers decentralized security features and load-sharing capabilities. However, adopting Blockchain in 5G-AKA has performance and latency concerns. Previous research has examined different types of Blockchains, such as public, private, consortium, and hybrid, but each has limitations in scalability, power consumption, or device capability. The consortium Blockchain architecture is considered most suitable, but it still faces performance consistency issues. Resolving these challenges requires considering a dynamic-size Blockchain approach [13-16].

The primary objective of this research paper is to enhance the performance of Blockchain-based authentication in 5G-AKA through the integration of an appropriate Blockchain design. This paper explores an innovative approach that leverages dynamic-size Blockchains to address performance consistency challenges in securing the SN-HN channel in 5G-AKA. This approach aims to optimize system performance under normal traffic conditions while ensuring a robust, consistent solution.

2. RELATED WORK

This section reviews the related research papers that have adopted Blockchain technology in 5G communication or related fields.

Salahdine et al. [17], in a review paper, examined 145 research articles in the field of 5G security. The study analyzed the risks associated with the 5G communication network, emphasizing that security breaches in 5G technology can be both expensive and complicated. The researchers encouraged the adoption of innovative technology enablers, primarily Blockchain. Blockchain demonstrated promise in enhancing system security, device compatibility, and load balancing, which primarily reduced catastrophic node failures. They also recommend adapting "Artificial Intelligence" and "Machine Learning" to enhance the network performance and to use defense-in-depth to secure each part of the network.

Dhar Dwivedi et al. [18] intensively investigated the adoption of Blockchain in 5G networks. Researchers explored the adaptability of Blockchain in IoT security due to its inherent security features. 5G-StandAlone (5G-SA) can easily integrate various IoT devices to boost network capacity and security.

Yadav et al. [19] developed a Blockchain-based approach to secure 5G-AKA authentication. The researchers demonstrate the 5G-AKA protocol and its deficiencies. Researchers employed Blockchain and elliptic curve encryption to bypass these constraints. The authors evaluated the performance of their system using Scyther and Real-Or-Random logic verifiers. The researchers found that the suggested protocol provides enhanced security and immutability for all types of attacks. The researchers also measured system performance by assessing communication costs, concluding that there was a considerable reduction in these costs. All these factors demonstrate that their framework enhances the security of the AKA mechanism.

A novel Blockchain-based AKA (BC-AKA) technique was created by Xiao and Gao [20] for the 5G Core network. The authors advocate for Blockchain-based decentralized authentication to enhance system security. Blockchain's basic features provide immutability by preventing single points of failure. The authors suggested using public Blockchains to enhance 5G network authentication and key distribution, according to this paper. Public-Blockchain enhanced AKA mechanism. The researchers recommend installing this system and monitoring its efficacy in real time rather than using a simulation tool.

Alkhateeb et al. [21] analyzed the adaptation of hybrid Blockchain to enhance the security of IoT devices by conducting a systematic review. The research addressed the flaws in the hybrid Blockchain. Researchers found that the hybrid technique improved system security. The researchers analyzed the rising global demand for IoT devices and the need to address their limitations, including the vast amounts of data, high energy consumption, and concerns about trust. Blockchain was suggested to address these difficulties.

The researchers utilized the Ethereum Blockchain network

to simulate transactions, recommending the use of a public Blockchain. The final examination revealed that the new technique improved security and process automation, but also increased latency and power consumption. Finally, the researchers encourage having more research to overcome latency and power consumption constraints [22].

The research paper by Hojjati et al. [23] describes a Blockchain-based 5G roaming AKA system. The updated protocol addresses 5G security challenges by leveraging the Blockchain's inherent features: transparency, interoperability, and decentralization. Blockchain technology provides transparent records, a decentralized architecture, and the ability to prevent DoS and DDoS attacks. The protocol protects user privacy and verifies the identities of all participants. Security is ensured through formal verification, particularly with ProVerif.

In their article, Hewa et al. [24] proposed using Blockchain technology to revoke certificates in 5G IoT networks. Certificate revocation invalidates compromised certificates, reducing the danger of unauthorized access and damage. The authors examined the challenges of revoking 5G IoT certificates.

2.1 Research limitations

Researchers have investigated diverse types of Blockchain networks, including public, private, consortium, and hybrid Blockchains, to secure the channel between SN and HN. However, each type of Blockchain network has its limitations and trade-offs. But the most important concern was the system performance, as measured by transaction throughput, latency, and resource consumption, which is a critical indicator for evaluating the effectiveness of securing the SN-HN channel. Considerations such as block and transaction sizes, as well as block time, significantly impact transaction throughput. This leads to a gap in system performance, where inconsistencies exist between peak and off-peak hours, and a need to ensure a secure and effective link between SN and HN in the 5G-AKA protocol. The researcher's contributions regarding the performance of the adopted Blockchain:

(1) The first group of researchers focused on transaction size as the primary factor for enhancing system performance. Configuring a small block size during off-peak hours increased throughput, but led to delays during peak hours with a high number of transactions [23].

(2) The second group focused on the block size as the primary factor for improving system performance. Configuring a high block size improved processing efficiency during peak hours, but resulted in unacceptable transaction delays for low transaction volumes [25, 26].

Table 1 below summarizes the research gaps and state of the art in securing the authentication mechanism using Blockchain in 5G-AKA.

Table 1. Summary of reviewed research on enhancing the Authentication and Key Agreement (AKA) mechanism through blockchain technology

Reference	Main Contribution	Type of Blockchain	Block Size	Number of Transactions per Block	Low Traffic	Normal Traffic	High Traffic
[18]	Use Blockchain to ensure IoT privacy-broadcast problem	Consortium Blockchain	NS	NS	NM	NM	NM
[19]	Use Blockchain to enhance 5G-AKA.	Public Blockchain	NS	NS	NM	NM	NM
[22]	Used Blockchain to provide Zero-Trust authentication.	NS	NS	NS	NM	NM	NM
[23]	Use Blockchain to enhance 5G-AKA.	Public Blockchain	1 MB	NS	NM	Depends on the level of congestion	H
[25]	Utilize Blockchain-based technology to enhance 5G-AKA.	Private Blockchain	1 MB	As per operator config (almost 2000 TPS)	L	Depends on the level of congestion	H
[26]	Use Blockchain to ensure HetNet privacy.	Private Blockchain	NS	NS	L	L	L
[27]	Use Blockchain to ensure IoT privacy.	Diverse types of Blockchain	NS	NS	H	H until 50 TPS	L
[28]	Use Blockchain to enhance 5G-AKA.	NS	NS	NS	NM	Depends on the level of congestion	H
The proposed framework	Enhance 5G-AKA by applying ECDH and Blockchain.	Consortium Blockchain	Dynamic	Dynamic	H	H	H

Note: NS: Not specified, NM: Not measured, H: High performance, L: Low performance, TPS: Transactions per second.

3. METHODOLOGY

The proposed methodology aims to determine the relationship between the block transaction count and system performance across varying levels of network congestion. The research is conducted across three main phases that test different network conditions: offloaded network, normal traffic volume, and congested network. For each of these conditions, three experimental configurations are evaluated: one transaction per block, a fixed block size of 1 MB, and a dynamic block size.

The experiments combine empirical testing and system modeling to comprehensively analyze performance variations across different network conditions and block sizes. Figure 2 illustrates the framework methodology. In this methodology, the subscribers and IoT devices with USIMs join the network.

Since these devices are not Blockchain users, they will submit queries as normal. To trigger the network, the Blockchain client, Next Generation Node B (gNodeB), which is equivalent to a base station, will initiate Application Programming Interface (API) queries to the network. The Caliper benchmark tool will generate typical queries and assess Blockchain performance from the client side.

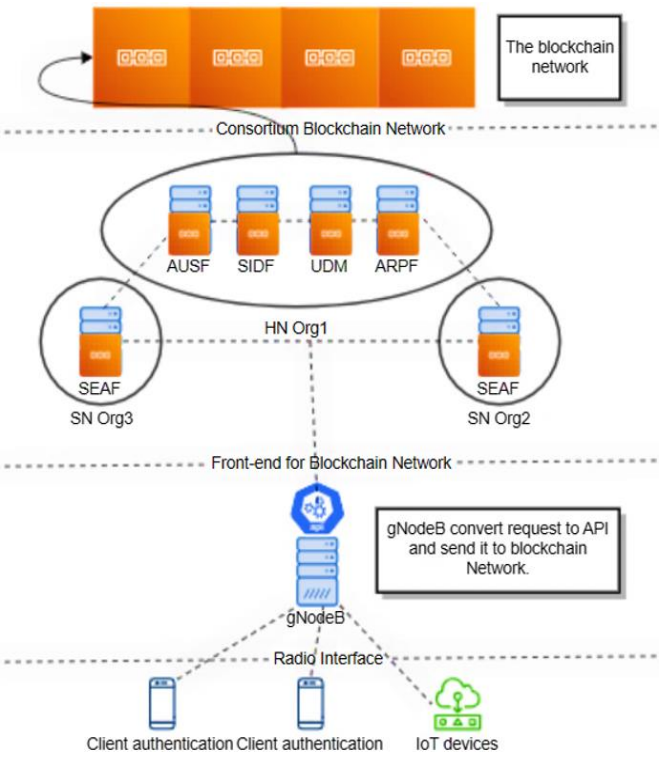

Figure 2. The proposed framework for the consortium Blockchain

The consortium Blockchain consists of the core 5G network functions defined by the 3GPP architecture. These include the Security Anchor Function (SEAF), responsible for key derivation and anchor security during authentication; the Authentication Server Function (AUSF), which performs authentication procedures; the Unified Data Management (UDM), which stores subscriber profiles; the Subscriber Identifier De-concealing Function (SIDF), which protects subscriber identity privacy; and the Authentication Credential Repository and Processing Function (ARPF), which manages authentication credentials at the HN. These entities collectively form the consortium Blockchain network and participate in block validation, with approved blocks being committed only after consensus is reached by the orderer nodes. The functional roles of these entities follow the 3GPP 5G system specifications [3GPP TS 23.501, TS 33.501].

To implement the suggested platform and simulate the experiment, Hyperledger Fabric has been chosen due to its phenomenal characteristics in permissioned Blockchain technology. The network was implemented from scratch, consisting of three organizations and a customized chaincode, and was integrated with Hyperledger Caliper, which serves as a client that generates customized requests and measures the network's performance. This broadcasts the transaction status to all associated nodes. The gNodeB sends the transaction response to the device via radio interface using standard signaling after receiving the update.

3.1 System and tools requirements

The experimental setup was designed to ensure reproducibility and accurate benchmarking of the proposed Blockchain framework. The hardware and software resources, as well as the tools used, are described below.

3.1.1 Hardware and operating system configuration

All experiments were conducted on a virtualized environment using Oracle VirtualBox (version 7.0) with a guest operating system of Ubuntu 22.04 LTS (64-bit). The host device specifications are summarized in Table 2, while the virtual machine configuration used for running the experiments is shown in Table 3.

Table 2. The specification of the device

Parameter	Specification
"Processor"	"12th Gen Intel (R) Core (TM) i5-1235U 1.30 GHz"
"Installed RAM"	"16.0 GB (15.7 GB usable)"
"System type"	"64-bit operating system, x64-based processor"

Table 3. Operating system specifications

Parameter	Specification
Operating System	Ubuntu 64-bit
Base Memory	10769 MB
Processors	8 CPU
Video Memory	16 MB
Allocated Storage	100 GB

3.1.2 Tools and software components

Hyperledger Fabric (Version 2.2) was used to configure the consortium Blockchain. The following prerequisites and tools were installed:

- Docker and Docker Compose containers- used to containerize applications and create isolated environments for each application.
- The Go, Python, Java, and Java Development Kit (JDK) libraries.
- NodeJS, Eclipse, and Gradle integration tool to package the Java chaincode and to interact with the Java Software Development Kit (SDK).
- Install the fabric binaries (fabric release 2.2 and binaries version 1.5.4) most stable version that can interact with caliper version 0.5.0.

Hyperledger Caliper to measure the metric performance and to work as a client.

- Install Hyperledger caliper Docker and CLI version 0.5.0, then bind the Caliper with the Fabric version 2.2. And configure (benchmark, workload, and networks) to generate the needed report that contains: throughput, latency, and resource consumption.

4. METRICS AND EVALUATIONS

Through analyzing the related work, where many researchers have adapted Blockchain to enhance the security of this communication channel. The experiments compared the suggested (dynamic) method to other researchers' approaches, which have a fixed block size. Due to those three experiments have been designed:

(1) The first experiment generates a single-transaction block.

(2) In the second experiment, a block is formed when the size surpasses 1 MB.

(3) The third experiment dynamically sizes blocks based on 100 transactions or a second wait time.

In all experiments, the performance, latency, and CPU utilization of the system under off-peak, peak, and normal traffic distributions have been measured. This assessment involves many rounds to ensure accuracy and consistency.

Performance Evaluation is the primary process for assessing the configured system's performance and efficiency by combining key parameters, including throughput measured in transactions per second (TPS), Latency measured in seconds, resource consumption in terms of allocated memory, and CPU utilization. In addition to the number of successful and failed transactions. The goal of this process is to evaluate the efficiency and the applicability of the designed platform.

(1) Transaction: The interaction between the client and the Blockchain network, usually this interaction can hold a wide variety of actions that are committed or discarded as per the defined business logic.

(2) Transaction Latency: This parameter is measured in seconds and represents the time difference between invoking the transaction and committing it (i.e., adding the transaction to the broadcasted block) when the transaction is approved in the network, as demonstrated in Eq. (1). This parameter is calculated per transaction, and Caliper can provide minimum, maximum, and average values in case multiple transactions are submitted to the system.

$$Latency = Confirmation\ timework - submit\ time \quad (1)$$

(3) Throughput: this parameter is measured in TPS, and it represents the number of validated transactions approved by the System Under Test (SUT) for a specific period. This parameter represents the overall network performance, taking into account that the number of invalid transactions will be subtracted from the total transactions in the calculation procedure, as shown in Eq. (2).

$$\text{Throughput} = \frac{Total\ committed\ transaction}{Total\ time\ in\ seconds \times number\ of\ committed\ nodes} \quad (2)$$

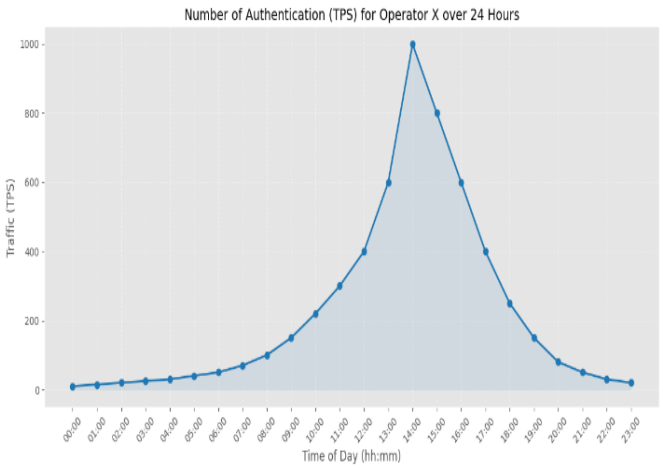

Figure 3. Number of authentication (TPS) distribution over 24 hours

The 24-hour TPS for one of the telecom operators is shown in Figure 3. The non-peak traffic is 5–50 TPS. The traffic volume ranges from 50 to 500 TPS in a typical network traffic distribution. The traffic might reach 900–1000 TPS during peak hours. To test system speed, latency, and CPU use, the Calliper ran 24 repetitions per experiment.

Below are the customizable solutions from Hyperledger Fabric, designed to build our system. Figure 4 shows the details of the applied system.

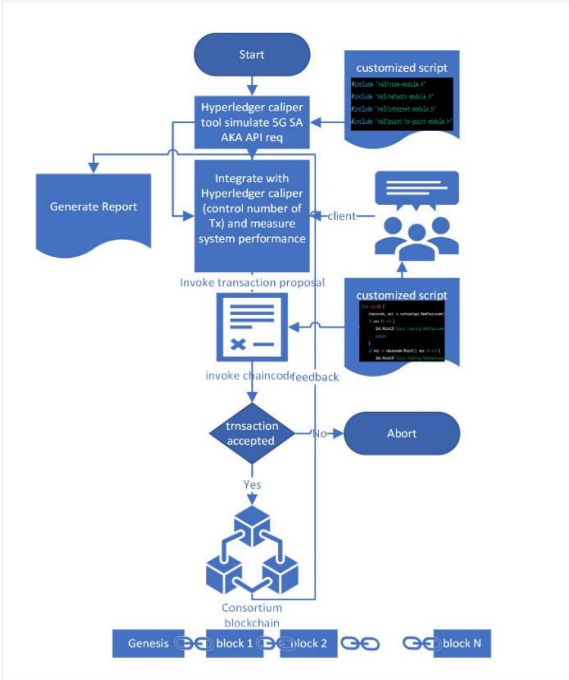

Figure 4. Hyperledger fabric system design

5. RESULTS

This section provides the results for the three experiments.

5.1 First experiment (one transaction per block experiment)

As illustrated in Figure 5, this experiment found that during the off-peak hours, the system generates 5–50 TPS. The system successfully handles all the transactions, and the latency was within typical parameters. When traffic gets higher, between 50 and 500 TPS, this experiment starts to fail. Multiple transactions were aborted due to timeout abort errors because the transaction's authentication procedure exceeded 5 seconds. Between 100 and 500 TPS, a bottleneck reduced throughput and success rates. Additionally, CPU use was considerable. The system performed poorly under network traffic congestion. This leads to a very low throughput and no success rate. The average delay was 31.5 seconds, and the resource utilization was around 100% at this level.

Conversely, network congestion resolution takes longer when traffic declines. This suggests that the network's real performance is not immediately apparent when traffic drops after congestion. All traffic is aborted, and delays are higher than when the network is offloaded. The network stabilizes when the load drops dramatically, resulting in a high success rate after offloading.

This confirms the hypothesis that this technique would

function best in non-congested networks. When network congestion or typical traffic distribution occurs, throughput, latency, and resource utilization are predicted to decrease.

5.2 Second experiment (one MB block size experiment)

The consortium Blockchain generated a 1MB block, and the Caliper ran 24 cycles to simulate traffic for this trial. Find the number of authentication transactions needed for a 1MB block. The 5G standard is 33.501 TS. Based on standard calculation, the estimated packet size in 5G-AKA is 140 bytes. So, on average, including the header of the block, each block to reach 1 MB size should encompass 7483 authentication messages.

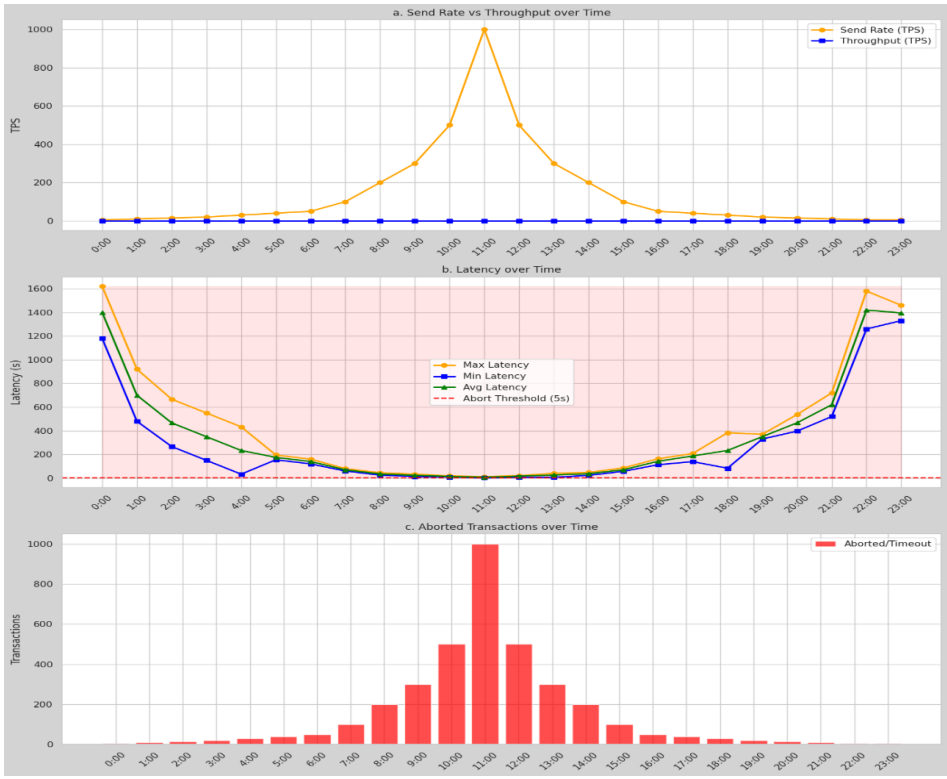

Figure 5. Comparison between input and output transaction throughput

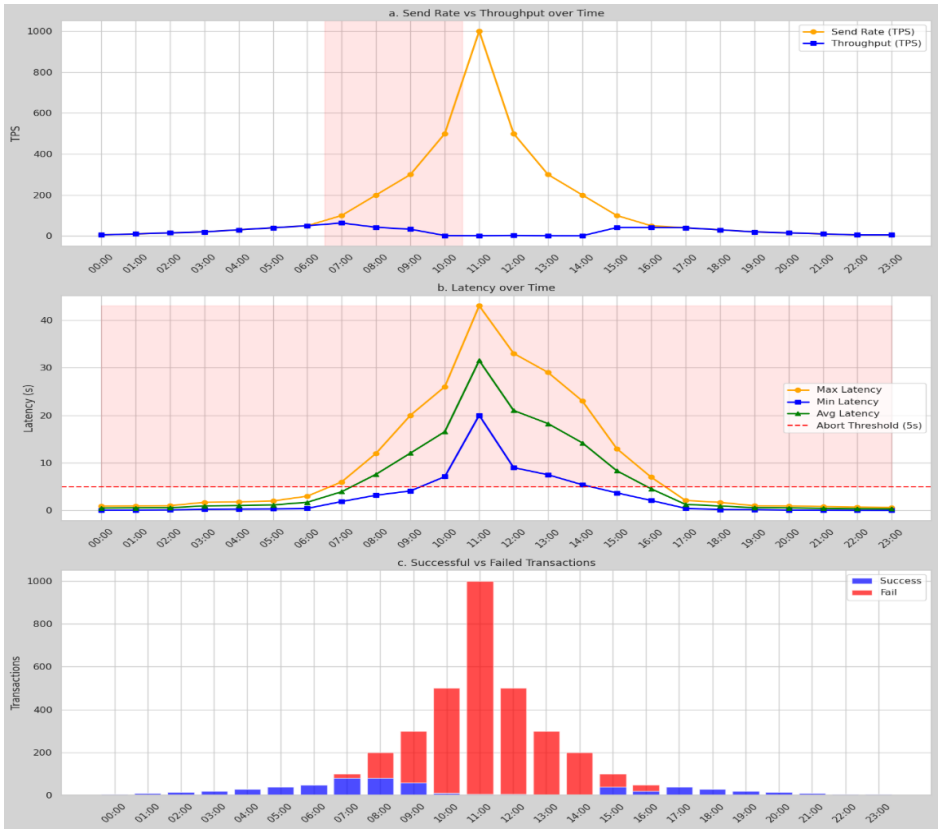

Figure 6. Comparison between input and output transaction throughput

Once the block size reached 1MB, the consortium Blockchain created the block, and the Caliper simulated one-day traffic with 24 cycles at different transmit speeds. A first test examined system performance with 5–50 TPS during off-peak traffic. A second test with 50–500 TPS assesses system performance under typical traffic distribution. The last assessment evaluates system performance at peak traffic, with 1,000 TPS. After deploying the chaincode and establishing the Caliper, it generated an HTML report with 24-test round performance, latency, and CPU consumption data at different TPS. Figure 6 compares 24-hour system performance with 1MB Blockchain blocks. Throughput was 0 during the testing, and no transactions were completed (all returned with a timeout abort error). This approach did not allocate traffic in a normal manner.

Off-peak traffic at 10 TPS takes 748 seconds to construct a block, or 12 minutes and 28 seconds. If the system produces 100 TPS with average traffic distribution, a block takes 75s. If the network is congested and produces 1,000 TPS, a block takes 7.5 seconds. Block time generation always exceeds the timeout, resulting in transactions being aborted.

5.3 Third experiment (dynamic block size experiment)

The consortium Blockchain generated blocks based on two criteria that met initially throughout this experiment:

(1) Condition 1: 100 transactions performed.

(2) Condition 2: 1-second timeout

If the system does not collect 100 transactions within 1 second, a block will still be generated to ensure uniformity and avoid latency. 24 rounds of the Caliper were run with varied transmit rates to simulate one day of traffic.

The first examination evaluated system performance during off-peak traffic, with 5-50 TPS. The second examination evaluates system performance under regular traffic distribution, with 50-500 TPS. The third examination evaluates system performance amid high traffic, with a TPS of about 1000.

This experiment demonstrated that the network failed to surpass the transaction barrier during off-peak hours. It started the block with a 1-second timer. Thus, during off-peak hours with 5–50 TPS traffic, the system generated a block every 1 second. This approach was used to process transactions with minimal delay during low traffic distribution, resulting in a 100% success rate and no abort timeout errors, as shown in prior trials. Since it created uniform blocks at the defined time threshold, the system's resource consumption was typical.

This experiment outperforms others in success. Before transaction traffic topped 100 TPS, time-limited block creation was used. Clearly, 100 TPS created a block per second. When traffic reached 200–500 TPS, the system started producing blocks with 100 transactions. Latency varied between the lowest and maximum values, giving the appearance of a decline in throughput. However, the system executed all transactions in under 5ms without any abort time problems. This time saw a rise in resource usage. CPU use increases under network traffic congestion. When the system gets 1000 TPS, it generates 10 blocks with 100 transactions each. However, 9 blocks were processed in less than 5 seconds, while the last block took 7 seconds. Therefore, all transactions in the previous block timed out owing to this delay, as depicted in Figure 7.

Reverting to its intended function without bottlenecks stabilized the network fast. The result supports the hypothesis that this technique would perform better across network congestion levels in terms of throughput, latency, and resource consumption, even in situations with both congestion and regular traffic distribution.

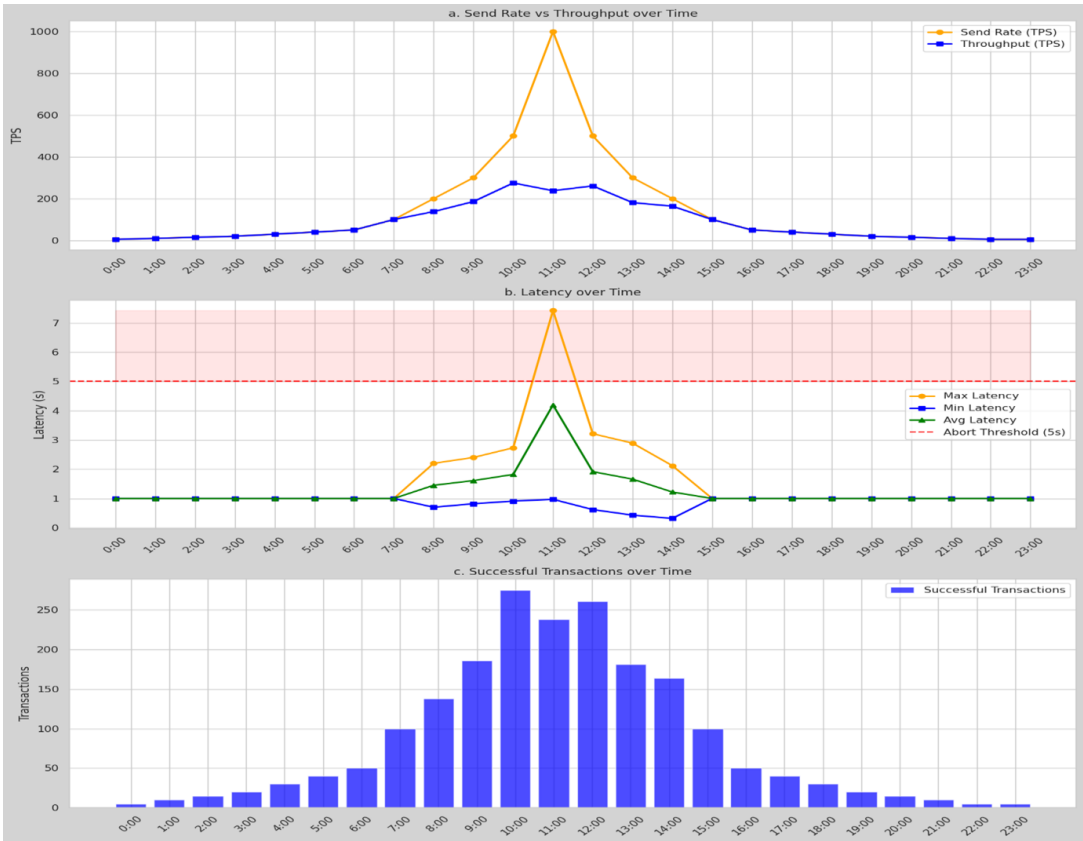

Figure 7. Comparison between input and output transaction throughput

6. DISCUSSION

In this section, we will assess the performance of the three experiments in the three predefined conditions for a telecom traffic pattern. Showing the performance evaluation under varying traffic load conditions.

6.1 First assessment (off-peak traffic) (5–50 TPS)

In this section, a comparison of the performance for the three experiments during off-peak traffic will be conducted, where the number of transactions varies between 5 and 50 TPS. Analyzing the information provided in Figure 8, it is evident that Experiment 3 (dynamic block size) achieved the highest level of performance, with a 100% success rate during off-peak traffic. This indicates that all submitted transactions were successfully processed within the standard time limit. Additionally, the network's performance was excellent when only one transaction was processed per block, resulting in a success rate of approximately 98.67% when the network was offloaded. However, when the number of transactions exceeded 50 TPS, a timeout error began to occur, drawing attention to the fact that the system was starting to face a bottleneck issue. As for the second experiment, the success rate was recorded as 0%, indicating that none of the transactions were authenticated, and all of them resulted in aborted timeouts. Based on the analysis, it can be concluded that the proposed approach demonstrates superior performance during periods of low traffic volume.

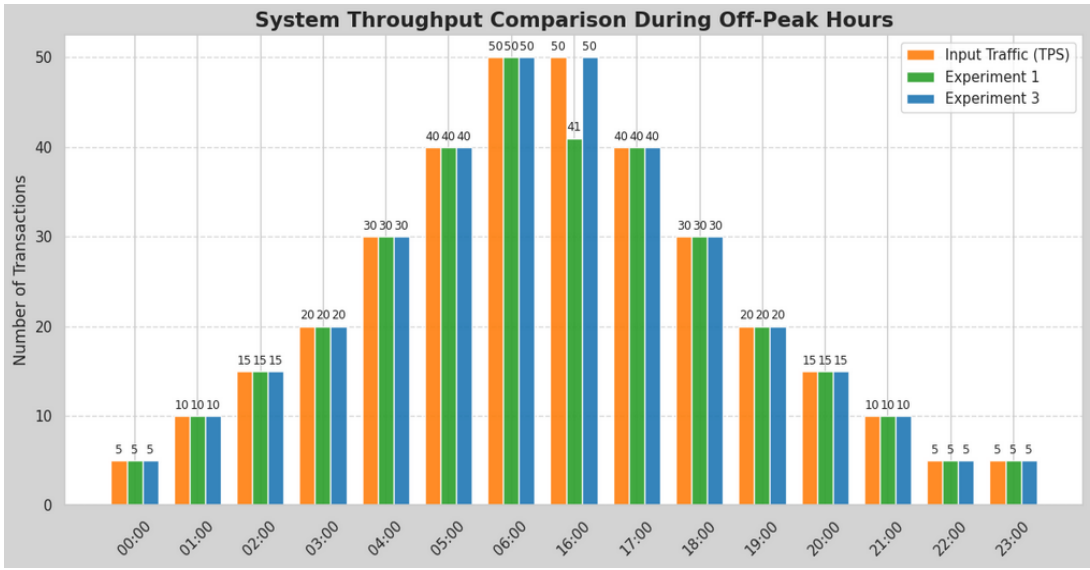

Figure 8. System throughput comparison during off-peak across experiments

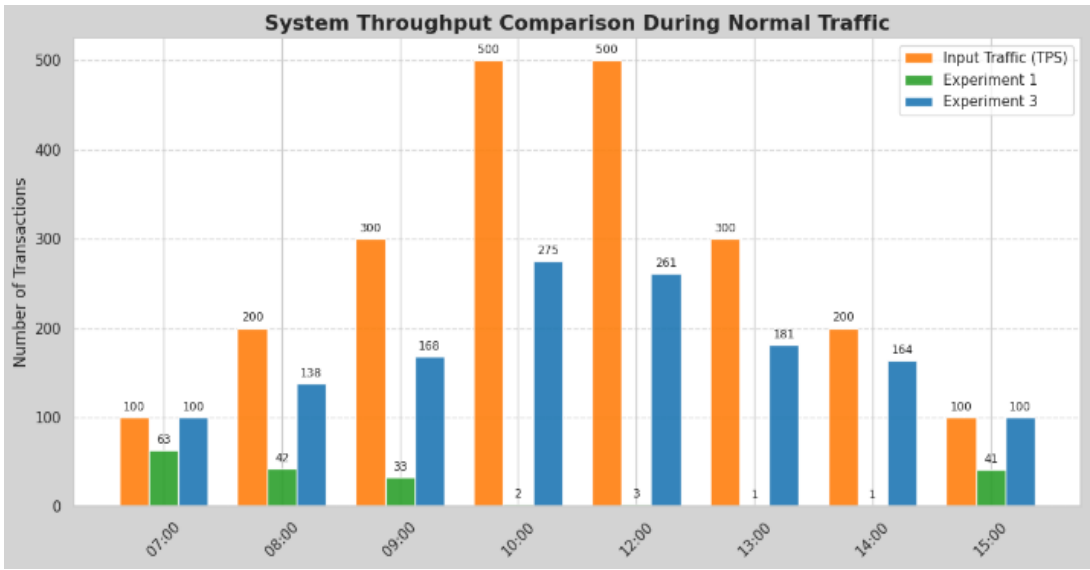

Figure 9. System throughput comparison during normal traffic across experiments

6.2 Second assessment (normal traffic distribution) (50 < TPS < 500)

In this section, the performance of the three experiments during normal traffic distribution will be compared, where the number of transactions varies between 100 and 500 TPS. Analysing the information provided in Figure 9, it becomes obvious that Experiment 3, which involved a dynamic block size, exhibited the most significant performance. This experiment achieved a 100% success rate, with approximately

72% of the submitted transactions being successfully processed within one second. However, other transactions were also successfully processed, but they experienced additional delays.

Even though the system itself introduced additional delays, it remained within the acceptable latency level as defined by the standard. In relation to Experiment 1, where each block consists of a single transaction, the system exhibited a performance drop due to a bottleneck problem. The system's throughput was below 17%, and almost all of the transactions were terminated due to timeout errors. Regarding the second experiment, which used a block size of 1MB, the success rate was observed to be 0%. This implies that none of the transactions were successfully confirmed within the specified time limit, resulting in all of them experiencing abort timeouts. This occurred because, up until that point, the block had not accumulated the required 7483 transactions necessary to generate a block. Based on the conducted analysis, it can be observed that the dynamic block size approach shows enhanced performance in instances characterized by standard traffic distribution.

6.3 Third assessment (peak traffic) (500 < TPS < 1000)

In this section, the performance of the three experiments during high traffic distribution will be compared, where the number of transactions is around 1000 TPS.

Upon a comprehensive examination of the data shown in Figure 10, it becomes evident that Experiment 3, which utilized a dynamic block size, demonstrated the most significant performance. The first conducted experiment demonstrated a minimal success rate, with a large number of transactions being terminated due to time constraints. Additionally, Experiment 2 had a success rate of zero because the network did not accumulate the required 7,483 transactions. Consequently, the transactions remained in the pool for an extended period, resulting in timeout errors. When evaluating various methodologies, the proposed method, which utilizes a dynamic block size, demonstrates superior performance across all scenarios, achieving a 90% success rate in highly congested networks. Even under these circumstances, the system maintains a high success rate in authenticating most transactions.

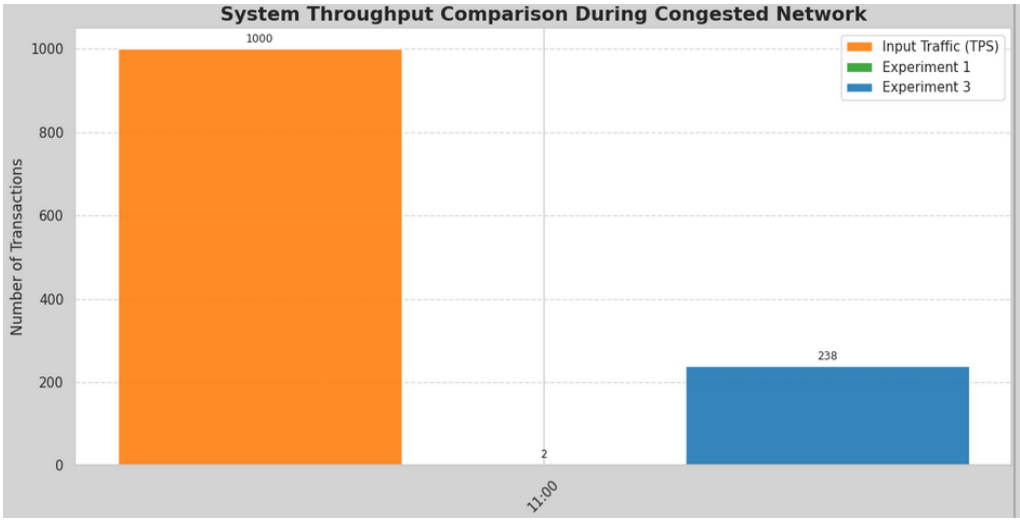

Figure 10. System throughput comparison during peak traffic across the experiment

6.4 Study limitation

One major limitation of Blockchain technology is its high resource consumption, which makes it unsuitable for IoT and handheld devices that struggle to maintain and synchronize the ledger. Future research should focus on developing lightweight mechanisms that enable these devices to participate efficiently in Blockchain networks. Additionally, integrating Blockchain with smart contracts offers promising opportunities to enhance roaming communication by automating authentication, agreement, and billing processes.

7. CONCLUSIONS

In conclusion, our framework offers significant optimization for protecting the communication channel between the HN and SN, utilizing Blockchain technology. The results emphasize the significance of employing a consortium Blockchain that has a dynamic block size creation methodology. This proposed framework demonstrated superior performance in terms of throughput, latency, and resource consumption when compared to previously recommended techniques. The dynamic block size technique demonstrated a success rate of 98%, whereas the fixed block size of 1 MB achieved a success rate of 0%. Additionally, when constrained to one transaction per block, the success rate was below 50%. Furthermore, in terms of latency, all fixed block size methods resulted in an unacceptable increase in transaction latency, while the dynamic block size approach succeeded in preserving the latency within the acceptable standardized level, not exceeding 5 milliseconds.

Based on a comprehensive analysis of the conducted experiments, it has become evident that the proposed dynamic size approach demonstrates improved performance compared to the different strategies suggested by other researchers. Particularly, the innovative approach aligns with real-life traffic patterns, thereby enabling its practical application in securing the communication channel between the SN and HN. The research findings are expected to have a significant impact on the development of 5G and future generations of telecommunication. This research is expected to inspire further investigation in this promising field. The knowledge acquired from this study can serve as a foundation for ongoing exploration and progress in the adoption of Blockchain technology in the context of 5G.

REFERENCES

[1] Al-Hamami, W.A., Ghrabat, M.J.J., Al-Hamami, M.A. (2024). Empowering optimizing resource management in 5G telecommunication networks: The power of machine learning. In 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain, pp. 251-257. https://doi.org/10.1109/ICETSIS61505.2024.10459366

[2] Aldehim, G., Khan, S., Shahzad, T., Khan, M.A., Ghadi, Y.Y., Jiang, W., Mazhar, T., Hamam, H. (2025). Balancing sustainability and security: A review of 5G and IoT in smart cities. Digital Communications and Networks, 11(6): 1722-1737. https://doi.org/10.1016/j.dcan.2025.06.007

[3] Narciandi-Rodriguez, D., Aveleira-Mata, J., García-Ordás, M.T., Alfonso-Cendón, J., Benavides, C., Alaiz-Moretón, H. (2025). A cybersecurity review in IoT 5G networks. Internet of Things, 30: 101478. https://doi.org/10.1016/j.iot.2024.101478

[4] Basin, D., Cremers, C., Dreier, J., Sasse, R. (2025). Case study: 5G-AKA. In Modeling and Analyzing Security Protocols with Tamarin. Information Security and Cryptography, pp. 195-214. https://doi.org/10.1007/978-3-031-90936-8_12

[5] Sultan, N.H., Guan, X., Pieprzyk, J., Ni, W., Abuadbba, S., Suzuki, H. (2025). Active attack resilience in 5G: A new take on authentication and key agreement. arXiv preprint arXiv:2507.17491. https://doi.org/10.48550/arXiv.2507.17491

[6] Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., Stettler, V. (2018). A formal analysis of 5G authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, pp. 1383-1396. https://doi.org/10.1145/3243734.3243846

[7] Joudah, R.H., Manaa, M.E. (2024). A new approach to improving the security of the 5G-AKA using Crystals-Kyber post-quantum technologies and ASCON algorithm. International Journal of Safety and Security Engineering, 14(6): 1729-1742. https://doi.org/10.18280/IJSSE.140608

[8] Yang, Y., Yang, G., Li, Y., Huang, M., et al. (2025). AKMA+: Security and privacy-enhanced and standard-compatible AKMA for 5G communication. In 34th USENIX Security Symposium (USENIX Security 25), pp. 5327-5345. https://www.usenix.org/system/files/usenixsecurity25-yang-yang.pdf.

[9] Kumar, N., Kumar, K., Aeron, A., Verre, F. (2025). Blockchain technology in supply chain management: Innovations, applications, and challenges. Telematics and Informatics Reports, 18: 100204. https://doi.org/10.1016/j.teler.2025.100204

[10] Jain, A.K., Gupta, N., Gupta, B.B. (2025). A survey on scalable consensus algorithms for blockchain technology. Cyber Security and Applications, 3: 100065. https://doi.org/10.1016/j.csa.2024.100065

[11] Senturk, O., Baghirov, A. (2024). The impact of blockchain technology on reducing cyber risks. Journal of Organizations, Technology and Entrepreneurship, 2(2): 122-135. https://doi.org/10.56578/jote020205

[12] Elomda, B.M., Abdelbary, T.A.A., Hassan, H.A., Hamza, K.S., Kharma, Q. (2025). An enhanced multi-layer blockchain security model for improved latency and scalability. Information, 16(3): 241. https://doi.org/10.3390/info16030241

[13] Khan, R., Kumar, P., Jayakody, D.N.K., Liyanage, M. (2020). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys & Tutorials, 22(1): 196-248. https://doi.org/10.1109/COMST.2019.2933899

[14] Shamaseen, A., Qatawneh, M., Elshqeirat, B. (2025). Blockchain for future smart grid: A comprehensive survey. Bulletin of Electrical Engineering and Informatics, 14(4): 2497-2513. https://doi.org/10.11591/eei.v14i4.8956

[15] Turab, N., Owida, H.A., Al-Nabulsi, J.I. (2024). Harnessing the power of blockchain to strengthen cybersecurity measures: A review. Indonesian Journal of Electrical Engineering and Computer Science, 35(1): 593-600. https://doi.org/10.11591/ijeecs.v35.i1.pp593-600

[16] Liu, Y.J., Zhang, L., Khadka, A. (2024). High-performance carbon cycle supply data sharing method based on blockchain multichain technology. Journal of Intelligent Management Decision, 3(2): 77-90. https://doi.org/10.56578/jimd030202

[17] Salahdine, F., Han, T., Zhang, N. (2023). Security in 5G and beyond recent advances and future challenges. Security and Privacy, 6(1): e271. https://doi.org/10.1002/spy2.271

[18] Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., Alnumay, W.S. (2024). Blockchain and AI for 5G-enabled IoT: Challenges, opportunities and solutions. Transactions on Emerging Telecommunications Technologies, 35(4): e4329. https://doi.org/10.1002/ett.4329

[19] Yadav, A.K., Braeken, A., Misra, M., Liyange, M. (2023). A provably secure and efficient 5G-AKA authentication protocol using blockchain. In 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, pp. 1110-1115. https://doi.org/10.1109/CCNC51644.2023.10059918

[20] Xiao, Y.L., Gao, S. (2022). Formal verification and analysis of 5G AKA protocol using mixed strand space model. Electronics, 11(9): 1333. https://doi.org/10.3390/electronics11091333

[21] Alkhateeb, A., Catal, C., Kar, G., Mishra, A. (2022). Hybrid blockchain platforms for the Internet of Things (IoT): A systematic literature review. Sensors, 22(4): 1304. https://doi.org/10.3390/s22041304

[22] Lin, W.X., Zhang, X.F., Cui, Q.M., Zhang, Z.W. (2021). Blockchain based unified authentication with zero-knowledge proof in heterogeneous MEC. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, pp. 1-6. https://doi.org/10.1109/ICCWORKSHOPS50388.2021.9473702

[23] Hojjati, M., Shafieinejad, A., Yanikomeroglu, H. (2020). A blockchain-based authentication and key agreement (AKA) protocol for 5G networks. IEEE Access, 8: 216461-216476. https://doi.org/10.1109/ACCESS.2020.3041710

[24] Hewa, T., Bracken, A., Ylianttila, M., Liyanage, M. (2020). Blockchain-based automated certificate revocation for 5G IoT. In ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, pp. 1-7. https://doi.org/10.1109/ICC40277.2020.9148820

[25] Chow, M.C., Ma, M. (2022). A secure blockchain-based authentication and key agreement scheme for 3GPP 5G networks. Sensors, 22(12): 4525. https://doi.org/10.3390/s22124525

[26] Shi, N., Tan, L., Li, W.J., Qi, X., Yu, K.P. (2021). A blockchain-empowered AAA scheme in the large-scale HetNet. Digital Communications and Networks, 7(3): 308-316. https://doi.org/10.1016/j.dcan.2020.10.002

[27] Jia, X.D., Hu, N., Yin, S., Zhao, Y., Zhang, C., Cheng, X.D. (2020). A2 chain: A blockchain-based decentralized authentication scheme for 5G-enabled IoT. Mobile Information Systems, 2020: 8889192. https://doi.org/10.1155/2020/8889192

[28] Haddad, Z., Fouda, M.M., Mahmoud, M., Abdallah, M. (2020). Blockchain-based authentication for 5G networks. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, pp. 189-194. https://doi.org/10.1109/ICIoT48696.2020.9089507