computation

MDPI

Article

Blockchain-Enhanced Security for 5G Edge Computing in IoT

Manuel J. C. S. Reis

Engineering Department & IEETA, University of Trás-os-Montes e Alto Douro, 5000-801 Vila Real, Portugal; mcabral@utad.pt

Abstract: The rapid expansion of 5G networks and edge computing has amplified security challenges in Internet of Things (IoT) environments, including unauthorized access, data tampering, and DDoS attacks. This paper introduces EdgeChainGuard, a hybrid blockchain-based authentication framework designed to secure 5G-enabled IoT systems through decentralized identity management, smart contract-based access control, and AI-driven anomaly detection. By combining permissioned and permissionless blockchain layers with Layer-2 scaling solutions and adaptive consensus mechanisms, the framework enhances both security and scalability while maintaining computational efficiency. Using synthetic datasets that simulate real-world adversarial behaviour, our evaluation shows an average authentication latency of 172.50 s and a 50% reduction in gas fees compared to traditional Ethereum-based implementations. The results demonstrate that EdgeChainGuard effectively enforces tamper-resistant authentication, reduces unauthorized access, and adapts to dynamic network conditions. Future research will focus on integrating zero-knowledge proofs (ZKPs) for privacy preservation, federated learning for decentralized AI retraining, and lightweight anomaly detection models to enable secure, low-latency authentication in resource-constrained IoT deployments.

Keywords: blockchain-based authentication; 5G edge computing; IoT security; scalability in blockchain; cybersecurity in IoT networks

check for updates

Received: 6 March 2025
Revised: 16 April 2025
Accepted: 17 April 2025
Published: 18 April 2025

Citation: Reis, M.J.C.S. Blockchain-Enhanced Security for 5G Edge Computing in IoT. *Computation* **2025**, *13*, 98. https://doi.org/10.3390/computation13040098

Copyright: © 2025 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The rapid proliferation of the Internet of Things (IoT) and the deployment of 5G networks have revolutionized data processing and service delivery. By enabling data processing closer to the source, edge computing reduces latency and enhances real-time decision-making capabilities. However, this shift introduces significant and domain-specific security challenges, including IoT device spoofing, data injection, and botnet-driven DDoS attacks that target authentication endpoints [1].

Traditional centralized security models often struggle to address these challenges due to inherent vulnerabilities, such as single points of failure, reliance on centralized identity providers, and limited scalability under high-load conditions. Blockchain technology, with its decentralized and tamper-proof characteristics, offers a promising solution for enhancing security in 5G-enabled edge computing environments. By integrating blockchain, it becomes feasible to establish decentralized identity verification, enforce smart contract-based access controls, and ensure immutable data integrity across IoT networks [2].

Several studies have explored blockchain's role in securing IoT ecosystems. For example, Bhat et al. [3] proposed a multi-tier edge–blockchain framework targeting lightweight security for constrained devices, and Zhang et al. [4] focused on decentralized access control for edge-based IoT networks. However, these models either lack scalability in high-load 5G scenarios or do not incorporate intelligent adaptation to dynamic threat patterns.

More recently, AI has been explored to enhance security analytics and threat detection in edge environments. Rathore et al. [5] demonstrated the use of deep learning for anomaly detection in 5G IoT, while Mollah et al. [6] proposed blockchain-enabled secure communication protocols for targeted message dissemination. These advances show promise but remain fragmented across layers and technologies.

This study proposes a unified architecture that integrates blockchain, AI, and edge computing to address these gaps. We introduce a novel hybrid blockchain framework, combining permissioned and permissionless chains for performance and security balance, enriched by AI-driven anomaly detection and Layer-2 scaling techniques for improved efficiency.

Unlike prior work, we focus on specific, high-impact security threats in 5G edge networks and validate our solution using synthetically generated authentication and transaction data that simulate real-world adversarial scenarios. Our goal is to provide both a theoretically grounded and practically deployable framework for IoT authentication in edge environments.

To address the limitations of existing authentication models in 5G-enabled IoT environments, this paper makes the following key contributions:

- Proposes a hybrid blockchain authentication framework that combines permissioned and permissionless blockchain models to balance security, decentralization, and computational efficiency in IoT edge computing.
- Introduces AI-driven adaptive consensus mechanisms to optimize transaction processing, anomaly detection, and security enforcement while reducing authentication latency.
- Incorporates Layer-2 scaling solutions (e.g., rollups, state channels, and sharding) to mitigate the transaction cost and scalability bottlenecks of blockchain-based authentication.
- Conducts an extensive performance evaluation, analysing transaction latency, computational overhead, and security resilience under different IoT network conditions using synthetic data simulations.
- Compares blockchain-based authentication with traditional models (e.g., OAuth, Kerberos) to highlight blockchain's advantages in tamper-proof identity verification and decentralized access control.
- Discusses future research directions in blockchain-based authentication, including zero-knowledge proofs (ZKPs), federated learning for decentralized security, and AI-optimized consensus models for enhancing scalability and privacy.

2. Related Work

The integration of blockchain into IoT and edge computing has attracted significant attention over the past decade, aiming to mitigate vulnerabilities such as data tampering, identity spoofing, and centralized failures. Recent work has focused on decentralized identity, data integrity, and access control, often leveraging lightweight consensus or fog computing [7–13]. Studies published between 2023 and 2025 have extended these applications to 5G IoT environments, but most still lack AI integration and rigorous performance evaluation under real-world 5G conditions. As a result, most approaches address isolated challenges, limiting their overall scalability and practical deployment.

This section categorizes existing contributions by functionality, identifies technical limitations, and positions our proposed hybrid framework as a unified, scalable solution that integrates blockchain, AI, and Layer-2 optimizations.

2.1. Decentralized Identity Management and Access Control

Blockchain's decentralized nature offers a robust framework for identity management in IoT networks. For instance, a study proposed a blockchain-based IoT device identification and management system within 5G networks, emphasizing decentralized

edge computing to enhance data security and identity authentication [14]. Similarly, the FogBus framework utilizes blockchain to provide a lightweight solution for edge and fog computing, ensuring secure operations on sensitive data [15]. Further, blockchain-based authentication schemes for collaborative edge computing environments have demonstrated enhanced security, particularly in resisting common IoT attacks [16]. In a broader context, Khan et al. [17] provide a detailed review of blockchain-based authentication systems in e-health, demonstrating how smart contracts, distributed ledgers, and data validation layers can collaboratively enforce access control and ensure immutability. Their findings underscore the versatility of blockchain authentication mechanisms across domains with high trust and privacy requirements, informing the cross-domain applicability of our proposed framework.

2.2. Data Integrity and Secure Computation Offloading

Ensuring data integrity and secure computation offloading are critical in IoT applications. A novel consensus algorithm, Proof of Authentication (PoAh), designed for large-scale IoT frameworks to maintain system sustainability and scalability while securing data, has been introduced [18]. Another study explored secure computation offloading in blockchain-based IoT networks using deep reinforcement learning, addressing the challenges of latency and energy consumption [19]. In addition, fog computing and blockchain-based security service architectures have been proposed to reinforce data protection within 5G industrial IoT cloud manufacturing environments [20].

2.3. Performance Evaluations in 5G IoT Environments

The performance and scalability of blockchain protocols in 5G IoT environments have been subjects of recent investigations. A comprehensive study compared various blockchain protocols, focusing on energy efficiency, transaction throughput, and latency, proposing potential solutions to improve these metrics [21]. Additionally, the Health-BlockEdge framework evaluated the performance and efficiency of integrating blockchain with edge computing in IoT models, considering factors such as latency, power consumption, and network usage [22]. Furthermore, a blockchain-enabled trusted authentication system for edge-based 5G networks has demonstrated promising results in reducing transaction delays and improving verification speed [13]. Nguyen et al. [23] provide a comprehensive survey on blockchain's role in enabling secure 5G technologies, including cloud and edge computing, highlighting key challenges and opportunities.

2.4. Advancements Towards Industry 5.0

The convergence of blockchain protocols and edge computing is pivotal in the transition towards Industry 5.0. A recent study highlighted how edge computing optimizes the performance of blockchain-based systems by reducing latency and improving response times, despite challenges related to security risks and adaptability [24]. Emerging solutions, such as blockchain-enabled multi-domain edge computing orchestration, offer improvements in collaborative resource sharing and security across distributed environments [25]. Xu et al. [26] provide a comprehensive taxonomy of blockchain-based systems, outlining key architectural trends that can be leveraged to build scalable and secure IoT infrastructures in 5G environments.

2.5. Security in Industrial IoT (IIoT) Systems

In the context of Industrial IoT, integrating edge computing with blockchain has been shown to enhance data security by processing information locally, thereby reducing the risk of data breaches. This integration facilitates real-time data analysis and decision-making at the network edge, which is crucial for industrial applications requiring swift

response times [27]. Security frameworks leveraging blockchain for IIoT authentication continue to evolve, with new lightweight RFID-based authentication protocols ensuring low-latency and tamper-resistant verification in mobile edge computing environments [28]. Additionally, blockchain-enabled authentication for vehicular edge computing (VEC) has demonstrated significant improvements in emergency message reliability and security [29], making it a viable approach for real-time IIoT security applications. Zhang et al. [30] demonstrated how blockchain can empower edge intelligence in 5G IIoT applications, optimizing distributed resource management and secure data processing. Gao et al. propose a blockchain-SDN-enabled Internet of Vehicles (IoV) framework for integrating fog computing in 5G networks, addressing security and privacy concerns in transportation systems [31].

2.6. Summary of Literature Review

Table 1 summarizes the key characteristics of recent blockchain-based security solutions for IoT and edge computing. While many frameworks address specific aspects like authentication or offloading, few offer integrated, performance-tested solutions tailored for 5G environments. Moreover, AI integration is often underexplored or entirely absent.

Table 1. Comparative summary of recent blockchain-based security frameworks for IoT and edge computing. The table highlights key features including blockchain type, AI integration, domain focus, and evaluation in 5G environments. The proposed work is distinguished by its integration of hybrid blockchain, AI-driven anomaly detection, and performance benchmarking under synthetic IoT conditions.

Study	Blockchain Type	AI Integration	Target Domain	5G Evaluation	Key Limitation
[2]	Permissioned	✗	Smart home IoT	✗	Early-stage, lacks scalability
[3]	Hybrid	✗	Edge computing	✗	No performance metrics
[5]	Public	✓ (DL)	5G IoT	✗	No Layer-2 scaling
[9]	Public	✓ (ML)	Generic IoT	✗	Limited scalability validation
[10]	Public + ZKP	Partial	Embedded IoT	✓	No adaptive consensus
[7]	Hybrid	✗	Large-scale IoT	Partial	No implementation details
[11]	Hybrid	✓ (AI + FL)	IIoT	✓	Complex integration
This work	Hybrid	✓ (CNN, LSTM)	5G IoT	✓	Uses synthetic data

3. Methodology

Our approach involves the design of a blockchain-based security framework, synthetic data generation for evaluation, and performance analysis. To provide a visual overview of the proposed security model, Figure 1 illustrates the architecture of our blockchain-integrated framework, highlighting its components across the IoT device layer, edge nodes, blockchain infrastructure, and AI-powered anomaly detection modules. The methodology consists of the steps described in the next subsections.

3.1. Security Threats in 5G Edge Computing for IoT

With the increasing deployment of 5G-enabled edge computing, IoT devices face a growing number of security threats that can compromise data integrity, availability, and authentication mechanisms. Traditional security solutions often rely on centralized models, which introduce single points of failure, making IoT networks vulnerable to attacks such as unauthorized access, data tampering, and DDoS attacks.

To systematically assess these risks, Table 2 presents a comparative analysis of the primary security threats, their impact levels, and how blockchain-based mechanisms provide mitigation strategies. Deep learning techniques have been combined with blockchain models to enhance threat detection in 5G IoT environments, as demonstrated

by Gumaei et al. [32], who applied these methods to drone identification and flight mode detection in real-time edge computing scenarios.

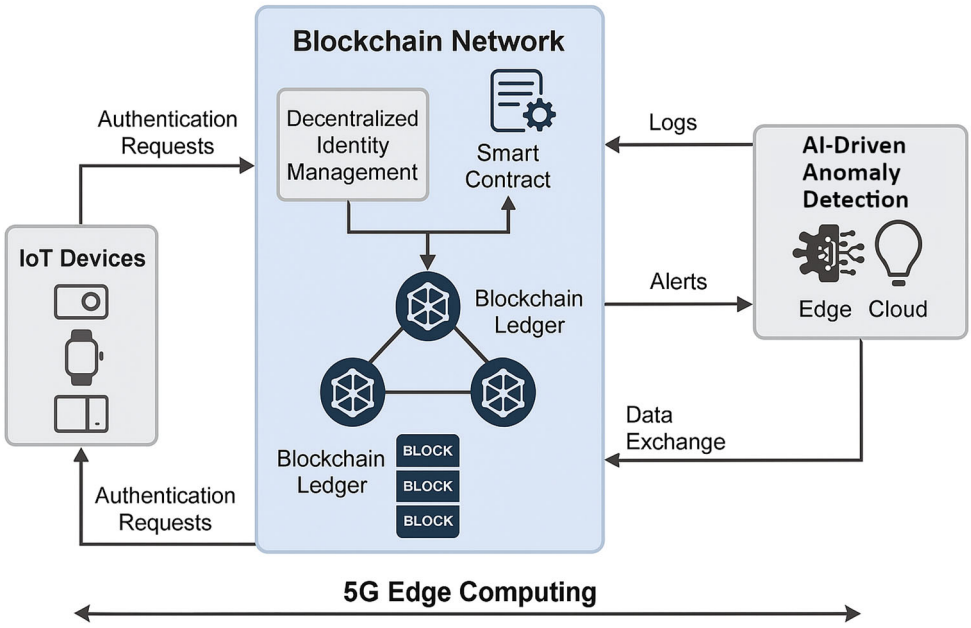


Figure 1. Proposed blockchain–AI security architecture for 5G-enabled IoT edge computing. The framework integrates decentralized authentication, smart contract-based access control, and AI-driven anomaly detection to mitigate security threats. It supports real-time transaction logging and adaptive policy enforcement across permissioned blockchain networks.

Table 2. Key security threats in 5G IoT edge computing.

Security Threat	Impact Level	Likelihood	Mitigation via Blockchain
Unauthorized Access	High	High	Decentralized authentication using blockchain-based identity verification.
Data Tampering	High	Medium	Immutable blockchain ledger ensures data integrity.
DDoS Attacks	Critical	Medium	Smart contracts limit repeated authentication requests, reducing attack vectors.
Single Point of Failure	High	High	Blockchain decentralization eliminates dependency on centralized servers.

3.1.1. Unauthorized Access and Authentication Failures

Unauthorized access is a major threat in IoT networks, as weak authentication protocols allow attackers to gain unauthorized control over edge devices. This can lead to data breaches, device manipulation, and large-scale cyberattacks.

To analyse this risk, we generated synthetic authentication logs containing both legitimate and malicious access attempts. The dataset revealed a failure rate of 47.2%, underscoring the high prevalence of unauthorized access attempts.

To illustrate this, Figure 2 presents the distribution of authentication success and failure rates among IoT devices. As seen in the figure, nearly half of all authentication attempts failed, highlighting the vulnerabilities in traditional authentication systems. By implementing blockchain-based authentication, we can significantly reduce failed authentication attempts by enforcing tamper-proof decentralized verification, improving security in 5G-enabled IoT networks. This figure illustrates how even in a synthetic model, fluctuating

success rates mirror the effects of adversarial patterns (e.g., brute-force spikes), validating the sensitivity of blockchain-based anomaly detection.

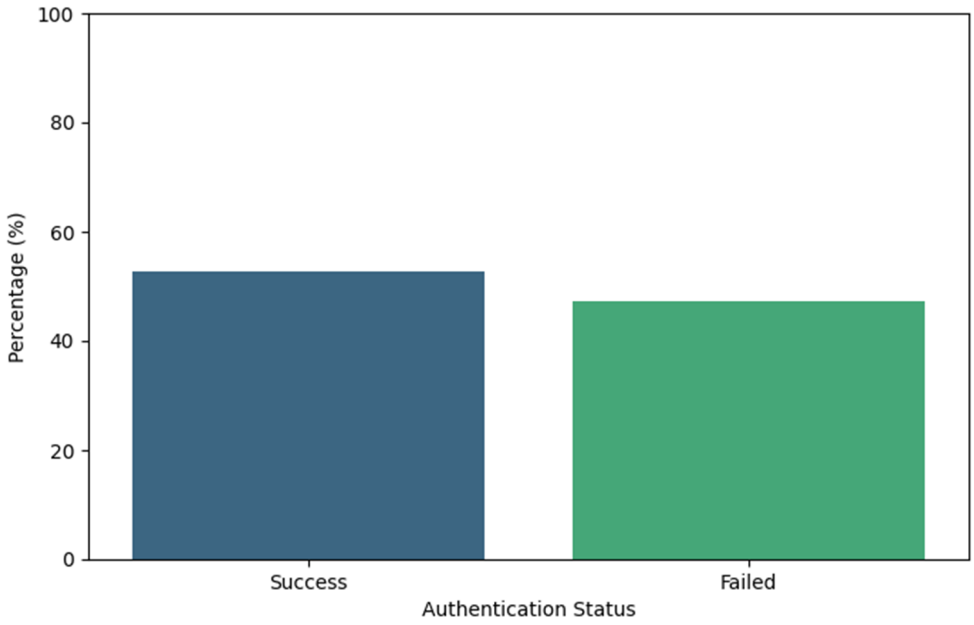


Figure 2. Authentication success vs. failure in IoT devices, based on a synthetic dataset designed to simulate real-world authentication behaviour under adversarial and benign conditions. Nearly half of all attempts failed, underscoring the vulnerabilities in traditional authentication. The distribution reflects the impact of adversarial patterns such as brute-force spikes, validating the sensitivity of blockchain-based anomaly detection.

As seen in Figure 1, nearly half of all authentication attempts failed, highlighting the vulnerabilities in traditional authentication systems. By implementing blockchain-based authentication, we can significantly reduce failed authentication attempts by enforcing tamper-proof decentralized verification, improving security in 5G-enabled IoT networks.

3.1.2. Data Tampering and Integrity Violations

Data integrity is critical for IoT security, particularly in healthcare, finance, and industrial applications. Attackers can intercept, modify, or inject malicious data into IoT systems, leading to compromised decision-making and potential financial or operational losses.

Hewa et al. [33] propose a multi-access edge computing (MEC) architecture integrating blockchain for privacy-preserving data storage in real-time telehealth applications.

While traditional hashing techniques can detect tampering, they do not prevent it. Blockchain's immutable ledger ensures that once data are recorded, they cannot be altered, providing trust and transparency in edge computing environments.

3.1.3. DDoS Attacks and Resource Exhaustion

Distributed Denial-of-Service (DDoS) attacks represent a critical threat in edge computing environments, particularly where IoT nodes and edge servers handle frequent, latency-sensitive authentication requests. Attackers can flood the system with a high volume of bogus authentication attempts, overwhelming bandwidth, depleting computational resources, and causing service interruptions or outages.

Traditional centralized authentication systems are especially vulnerable due to their reliance on single points of failure. When a central server becomes saturated, the entire network's authentication infrastructure can collapse, making it an attractive target for botnet-driven attacks.

Blockchain-based architectures address this issue by decentralizing authentication logic across multiple nodes. In our framework, smart contracts are used to enforce rate-limiting and access control policies directly on-chain. While rate limiting is not unique to blockchain and can be implemented in centralized systems as well, smart contracts enable a distributed enforcement of these rules, reducing the risk of system-wide failure if individual nodes are targeted.

It is important to clarify that smart contracts do not inherently prevent DDoS attacks. However, by distributing verification logic across the blockchain and eliminating reliance on a central authority, they reduce the overall attack surface. This decentralized structure makes it more difficult for adversaries to disrupt the authentication process at scale, thereby improving resilience in trustless and resource-constrained IoT environments.

3.1.4. Eliminating Single Points of Failure

Traditional centralized security models pose an inherent risk—if the main authentication server is compromised or disabled, the entire IoT network can be affected. Attackers exploit these vulnerabilities in centralized systems to launch targeted attacks on core infrastructure.

Blockchain, through its distributed nature, eliminates these risks by ensuring that no single entity controls authentication or access control policies. Instead, all authentication requests are validated through a decentralized consensus mechanism, making IoT networks more resilient and fault-tolerant.

3.2. Blockchain Integration for Security

To address the security challenges in 5G-enabled IoT edge computing, we propose a blockchain-based security framework that enhances authentication, access control, and secure data exchange. The framework leverages smart contracts, decentralized identity management, and anomaly detection to create a tamper-proof and resilient security model.

As illustrated in Figure 1, the proposed framework establishes a layered architecture in which IoT devices authenticate via permissioned blockchain nodes at the edge, while AI-driven anomaly detection modules continuously analyse transaction patterns to detect threats in real time. This integration enables secure access control, tamper-proof logging, and adaptive response mechanisms across 5G-enabled environments.

3.2.1. Blockchain Network Architecture

The choice of blockchain architecture significantly impacts security, scalability, and energy efficiency. Two main types of blockchain networks are considered for IoT security, as shown in Table 3.

Table 3. Types of blockchain networks considered for IoT.

Blockchain Type	Characteristics	Suitability for 5G IoT Security
Permissionless Blockchain	Fully decentralized, open to all participants, high transparency, requires high computational power (e.g., Bitcoin, Ethereum).	Not ideal for IoT due to high energy consumption and latency.
Permissioned Blockchain	Access restricted to trusted nodes, higher efficiency, customizable security policies (e.g., Hyperledger Fabric, Quorum).	Best for 5G IoT, as it balances security, performance, and resource efficiency.

Since 5G-enabled IoT applications require low-latency authentication and controlled access, our framework adopts a permissioned blockchain model. This approach ensures that only trusted nodes participate in authentication while maintaining decentralization.

Traditional authentication models such as OAuth and Kerberos have been widely used in IoT and enterprise environments. However, their centralized nature introduces vulnerabilities, such as single points of failure, susceptibility to data breaches, and limited scalability. In contrast, blockchain-based authentication eliminates these risks through decentralized identity management. Table 4 provides a comparative analysis of blockchain authentication versus centralized authentication protocols, highlighting their strengths and limitations.

Table 4. Comparison of blockchain authentication vs. centralized authentication models.

Feature	Blockchain Authentication (e.g., Hyperledger, Ethereum)	OAuth (Centralized Token-Based)	Kerberos (Centralized Ticket-Based)
Security Robustness	High—Immutable ledger prevents tampering; cryptographic security ensures strong authentication	Medium—Tokens can be intercepted if not encrypted properly	Medium—Tickets are vulnerable to replay attacks and key theft
Single Point of Failure (SPoF)	None—Decentralized, reducing the risk of a single point of failure	High—OAuth relies on a centralized identity provider	High—Kerberos authentication server is a single point of failure
Tamper Resistance	High—All authentication transactions are cryptographically signed and immutable	Medium—Tokens are cryptographically signed; tampering is prevented unless encryption is weak or access tokens are leaked	Medium—Tickets can be replayed if not expired or if keys are compromised, though mitigated by time-stamped session tickets and short expiration windows
Scalability	Medium—Transaction speed depends on blockchain type (permissioned blockchains are more scalable)	High—OAuth scales efficiently in web and cloud services	High—Kerberos scales well for enterprise networks but struggles with large-scale IoT
Computational Overhead	Moderate—PoS significantly reduces energy cost compared to PoW, while PBFT introduces communication overhead but avoids heavy computation	Low—Lightweight authentication, but requires continuous token verification	Medium—Kerberos requires encryption but is optimized for corporate networks
Real-time Performance	Medium—Latency depends on blockchain consensus (e.g., 1–10 sec for Hyperledger, 10+ min for Bitcoin)	High—OAuth tokens enable fast authentication in milliseconds	High—Kerberos supports real-time authentication through pre-shared tickets
Privacy	High—Pseudonymous authentication; no central authority tracks credentials	Low—OAuth providers track user credentials and access logs	Low—Kerberos relies on a central key distribution centre (KDC), which can be compromised
Resistance to DDoS Attacks	High—Decentralized nodes reduce the impact of attacks	Low—Centralized servers are vulnerable to high-traffic attacks	Medium—Kerberos is vulnerable to KDC overload but uses ticket expiration as a mitigation

In our implementation, we simulate Hyperledger Fabric as the permissioned blockchain layer for local edge authentication, while Ethereum is modelled for tamper-proof public logging. Fabric's use of PBFT (Practical Byzantine Fault Tolerance) provides fast consensus for low-latency use, whereas Ethereum offers global consistency. The smart contract-based policies are written in Solidity and deployed in Ganache (local testnet) for evaluation.

3.2.2. Smart Contract-Based Access Control and Enforcement

One of the key security challenges in IoT networks is ensuring that only authorized devices gain access to the network. Traditional centralized authentication models are

prone to spoofing attacks and single points of failure, making them unsuitable for 5G edge computing.

To address this, we integrate smart contract-based access control, where authentication policies are automatically enforced through immutable blockchain logic. The pseudo-code in Listing 1 illustrates how this process is implemented.

Listing 1. Pseudo-code for smart contract logic for IoT authentication.

```
pragma solidity ^0.8.0;
contract IoTAccessControl {
      mapping(address => bool) authorizedDevices;
      address owner;
      constructor() {
          owner = msg.sender;
      }
      function registerDevice(address device) public {
          require(msg.sender == owner, "Only owner can register
devices");
          authorizedDevices[device] = true;
      }
      function authenticateDevice(address device) public view returns
(bool) {
          return authorizedDevices[device];
      }
}
```

In this model, an IoT device attempting to authenticate queries the blockchain to verify whether its identity is registered. Because blockchain data are immutable and cryptographically secure, this eliminates the risk of forged identities or unauthorized modifications to access control policies.

Beyond the basic authentication shown above, our full implementation includes additional smart contract logic to support access rate limiting, transaction validation, and suspicious behaviour flagging. These functionalities interact with the AI-based anomaly detection module described in Section 3.2.4. Specifically, AI outputs (e.g., anomaly scores or flagged timestamps) are stored on-chain via auxiliary contracts that adjust access permissions or issue warnings dynamically. While omitted from the pseudocode for clarity, these extensions form the core enforcement mechanism in our prototype.

3.2.3. Secure Data Exchange

Beyond authentication, IoT devices must continuously exchange data with edge computing nodes while maintaining integrity, confidentiality, and availability. A significant challenge arises when malicious actors attempt to intercept or modify transmitted data, leading to misinformation, system compromise, or privacy breaches. According to Zheng et al. [34], blockchain not only enables secure data sharing in IoT networks, but also provides a transparent mechanism for verifying data integrity, which is essential for edge computing in 5G environments.

By leveraging blockchain-based encryption and distributed ledger technology, our framework ensures the following:

- Tamper-proof Data Storage: Each transaction is cryptographically hashed and stored in blocks, preventing unauthorized modifications.
- End-to-End Encryption: Only authenticated IoT devices can decrypt and access transmitted data, ensuring data confidentiality.

- Efficient Gas Fee Optimization: Smart contracts execute only when required, minimizing computational overhead and transaction costs in resource-constrained IoT environments.

These mechanisms collectively enhance the security of real-time IoT communications without compromising performance.

3.2.4. Anomaly Detection Mechanisms

In addition to access control and data security, proactive threat detection plays a vital role in mitigating cyberattacks in 5G-enabled IoT networks. Blockchain transaction logs provide a valuable dataset for analysing patterns of authentication attempts and identifying malicious activities.

To improve real-time security monitoring, our framework integrates AI-driven anomaly detection alongside traditional rule-based security mechanisms. Table 5 provides a comparative analysis of these two approaches.

Table 5. Comparison of AI-based and traditional security mechanisms.

Method	Advantages	Limitations
Traditional Rule-Based Security	Simple implementation, deterministic decisions	High false positives, unable to detect evolving threats
AI-Based Anomaly Detection	Adaptive, detects complex attack patterns, real-time threat mitigation	Requires training data, computationally intensive

Unlike static rule-based policies, AI-driven models continuously learn and adapt to evolving security threats. For example, an anomaly detection system can undertake the following:

1. Analyse blockchain transaction patterns to detect unusual authentication requests.
2. Identify suspicious behaviour, such as repeated failed login attempts or rapid authentication requests from a single device.
3. Automatically trigger countermeasures, such as blocking unauthorized devices or flagging suspicious transactions for review.

By combining blockchain with AI-driven anomaly detection, we establish a self-adaptive security model that proactively prevents cyber threats while maintaining network efficiency. Nkenyereye et al. [35] introduced a secure blockchain-based emergency-driven messaging protocol for 5G-enabled vehicular edge computing, enhancing the reliability and security of real-time authentication mechanisms in IoT.

Traditional anomaly detection in blockchain relies on static rule-based mechanisms, which are often ineffective against evolving cyber threats. To enhance security, AI-driven models such as CNNs and LSTMs can be integrated with blockchain authentication to analyse transaction patterns in real time. These models can detect suspicious activity, including authentication anomalies, fraudulent transactions, and timing-based attacks. By leveraging AI, blockchain authentication becomes more resilient to emerging security threats while maintaining low false-positive rates.

AI-Driven Anomaly Detection for Blockchain-Based IoT Security

Blockchain's immutability and transparency make it well suited for security monitoring, but traditional rule-based security models struggle to detect sophisticated cyber threats such as zero-day attacks, data poisoning, and adversarial manipulations. To address these challenges, AI-driven anomaly detection can be integrated with blockchain-based authentication to enhance security in 5G IoT networks.

By analysing blockchain transaction patterns, machine learning (ML) models can detect suspicious authentication attempts, fraudulent transactions, and anomalous behaviours. This integration enables a real-time, self-learning security model that adapts to new threats without manual intervention. Table 6 presents a summary of AI models and their applications in blockchain-based IoT security.

Table 6. How AI can enhance blockchain security in IoT.

AI Model	How It Works	Use Case in Blockchain-Based IoT Authentication	Advantages
Convolutional Neural Networks (CNNs)	Learns spatial patterns in authentication transactions	Detects anomalies in blockchain logs based on transaction structure	Fast pattern recognition with high accuracy
Long Short-Term Memory (LSTM) Networks	Captures temporal dependencies in transaction sequences	Identifies suspicious repetitive authentication failures and timing-based attacks	Effective for sequential data in time-series blockchain records
Autoencoders	Learns normal behaviour and detects deviations	Flags deviations in blockchain authentication logs, reducing false positives	Self-learning, requires minimal labelled data
Random Forest and Decision Trees	Classifies transactions as normal or suspicious	Detects fraudulent blockchain activities with interpretable results	Low computational cost, effective for structured datasets
Reinforcement Learning (RL)	Continuously optimizes security rules based on attack patterns	Adapts authentication policies dynamically to minimize cyber threats	Self-improving, robust against evolving attacks

The CNN model consists of 3 convolutional layers (32, 64, and 128 filters) with ReLU activation, followed by a fully connected layer. The LSTM model includes two stacked LSTM layers with 128 hidden units each. Both models were trained on 70% of the synthetic dataset, validated on 15%, and tested on the remaining 15%. Feature vectors included transaction frequency, time between authentications, gas fees, and failed attempt count.

AI–Blockchain Integration for Real-Time Security Monitoring

To implement AI-driven anomaly detection, blockchain authentication logs can be fed into machine learning models to detect suspicious activities. The workflow consists of the following steps:

- Data Collection—Blockchain transaction logs and authentication records are continuously collected from edge nodes.
- Feature Extraction—The ML model extracts key features such as authentication timestamps, transaction frequency, gas fees, failed login attempts, and access patterns.
- Model Training—The extracted features are used to train CNNs, LSTMs, and Autoencoders to recognize normal vs. anomalous authentication events.
- Real-Time Anomaly Detection—Once deployed, the AI model monitors blockchain transactions and flags unusual activity in real time.
- Response Mechanism—Detected anomalies trigger smart contract-based security policies, such as automatically blocking suspicious IoT devices or triggering additional verification steps.

The final model used for anomaly detection was a two-layer stacked LSTM network, each layer with 128 hidden units, followed by a dense sigmoid classifier. Inputs consist of a time window of 10 consecutive authentication log entries (timestamp, gas fee, success/failure flag), normalized using MinMax scaling. The output is a binary anomaly score. The model was trained using the Adam optimizer (learning rate = 0.001), with early

stopping after 10 epochs of no validation improvement. Hyperparameters were tuned via grid search on a validation split (20%) from synthetic logs.

The LSTM model used for anomaly detection was trained on time-series authentication logs. Table 7 summarizes the model architecture and training configuration. A two-layer LSTM was selected based on performance benchmarking against CNNs and Autoencoders.

Table 7. Architecture and training details of the LSTM-based anomaly detection model.

Component	Description
Model Type	Long Short-Term Memory (LSTM) Neural Network
Architecture	2 stacked LSTM layers (128 units each) + 1 dense layer (sigmoid activation)
Input Features	Timestamp, gas fee, authentication outcome (success/fail), device ID
Input Format	Sliding window of 10 sequential transactions per sample
Output	Binary anomaly score (0: normal; 1: anomaly)
Loss Function	Binary cross-entropy
Optimizer	Adam (learning rate = 0.001)
Training Epochs	Max 100, with early stopping (patience = 10)
Hyperparameter Tuning	Grid search (batch size, window size, number of LSTM units)
Validation Split	20% of training data
Frameworks Used	TensorFlow 2.x, Scikit-learn

Example: Using LSTMs for Anomaly Detection in Blockchain Authentication

A Long Short-Term Memory (LSTM) model can be trained on historical blockchain authentication logs to predict malicious activity. If the LSTM detects anomalous behaviour (e.g., unusual transaction frequency, multiple failed authentications, sudden spikes in authentication requests), it can undertake the following:

1. Trigger a security alert in the blockchain network.
2. Dynamically update smart contract rules to require additional verification.
3. Isolate suspicious IoT devices from the authentication process.

This approach ensures adaptive security, where the blockchain network evolves based on detected threats rather than relying on static security rules.

3.3. Synthetic Data Generation

To evaluate the proposed model under realistic network dynamics, we constructed synthetic authentication logs and blockchain transaction sequences that reflect known adversarial behaviours and access patterns. These were designed using statistical distributions observed in real-world security logs, including diurnal access peaks, random authentication failures, and denial-of-service spikes. The dataset generation scripts and configuration parameters will be made publicly available upon publication to support reproducibility.

3.3.1. Dataset Composition

To ensure a realistic evaluation of our blockchain-based security framework, we generated a synthetic dataset that simulates authentication behaviours and blockchain transactions in a 5G-enabled IoT environment. While the dataset is synthetic, it is derived from real-world attack patterns and network behaviours observed in prior work (e.g., [1,36]). The parameters used—such as failure rates, DDoS request volumes, and authentication timeouts—reflect empirical norms found in production-grade IoT networks and academic evaluations. The dataset consists of two primary components:

1. IoT authentication logs, capturing both legitimate and malicious authentication attempts.
2. Blockchain transactions, documenting smart contract executions, access control decisions, and transaction success rates.

To provide a structured overview of the synthetic datasets used in our analysis, we present summary statistics of both blockchain transaction records and IoT authentication logs. Table 8 details the characteristics of the blockchain dataset, while Table 9 highlights key distributions within the IoT authentication dataset.

Table 8. Blockchain data summary.

Metric	Count	Mean	Std Dev	Min	25%	50% (Median)	75%	Max
Gas Fee (ETH)	500.0	0.005465	0.002642	0.001013	0.003206	0.005447	0.007808	0.009978

Table 9. IoT authentication data summary.

Metric	Count	Mean	Std Dev	Min	25%	50%	75%	Max
Latency (s)	500.0	172.50	177.86	0.00	44.00	115.00	236.50	1040.00
Success Rate (%)	500.0	52.80	49.97	0.00	0.00	100.00	100.00	100.00

The dataset reflects a real-world mix of normal and attack scenarios, ensuring that the security framework is tested under diverse conditions. Table 10 presents key statistics summarizing the dataset composition.

Table 10. Key statistics of the synthetic dataset.

Parameter	Value
Total Authentication Attempts	500
Successful Authentications	52.8%
Failed Authentications	47.2%
Total Blockchain Transactions	500
Attack Simulation Percentage	30%

By analysing this dataset, we can assess how effectively blockchain authentication mechanisms mitigate unauthorized access attempts, resist DDoS attacks, and maintain secure transaction integrity. The failure rate of 47.2% highlights the security challenges in IoT environments and the necessity for decentralized authentication solutions.

Synthetic datasets were chosen to enable controlled testing across diverse adversarial scenarios, reflecting observed patterns from production IoT networks. While synthetic data provide a controllable testbed, future work will involve validation using real-world IoT traffic datasets to assess generalizability.

3.3.2. Attack Simulation Process

To evaluate the resilience of our framework, we introduced multiple types of cyber threats into the dataset:

(a) Unauthorized Access Attempts:

- Simulated brute-force login attempts, where an attacker repeatedly tries incorrect credentials to gain access.
- Modelled device spoofing attacks, where a rogue device pretends to be a legitimate IoT node.

(b) DDoS Authentication Flooding:

- Introduced high-frequency authentication requests from malicious nodes to simulate a DDoS attack targeting authentication servers.
- Evaluated how smart contract-based access control limits excessive login requests to mitigate DDoS attacks.

(c) Blockchain Transaction Manipulation:

- Simulated malicious smart contract interactions, including unauthorized modifications of access control policies.
- Tested blockchain's resistance to double-spending attacks, ensuring the immutability of transaction records.

These attack simulations provided a controlled testing environment to measure blockchain's ability to prevent authentication failures and detect anomalies.

The selection of these attack types is based on their critical impact on 5G-enabled IoT security. Unauthorized access attacks compromise authentication integrity, allowing adversaries to hijack IoT devices or access sensitive data. DDoS authentication flooding disrupts service availability by overwhelming authentication servers, degrading network performance in real-time applications. Meanwhile, blockchain transaction manipulation threatens the integrity of authentication logs, allowing malicious actors to alter or forge access control decisions. These threats represent some of the most significant cybersecurity risks in IoT environments, making them essential test cases for evaluating the effectiveness of our blockchain-based security framework. By simulating these attack types, this study evaluates the resilience of the proposed hybrid blockchain authentication model against real-world cyber threats, ensuring that the framework can effectively mitigate critical security risks in 5G IoT applications.

3.3.3. Data Distribution and Visualization

To analyse the behaviour of authentication attempts over time, we present Figure 3, which illustrates the evolution of authentication success rates throughout the dataset. By computing a rolling success rate, we observe fluctuations in authentication performance, highlighting periods of increased failure rates and potential security vulnerabilities.

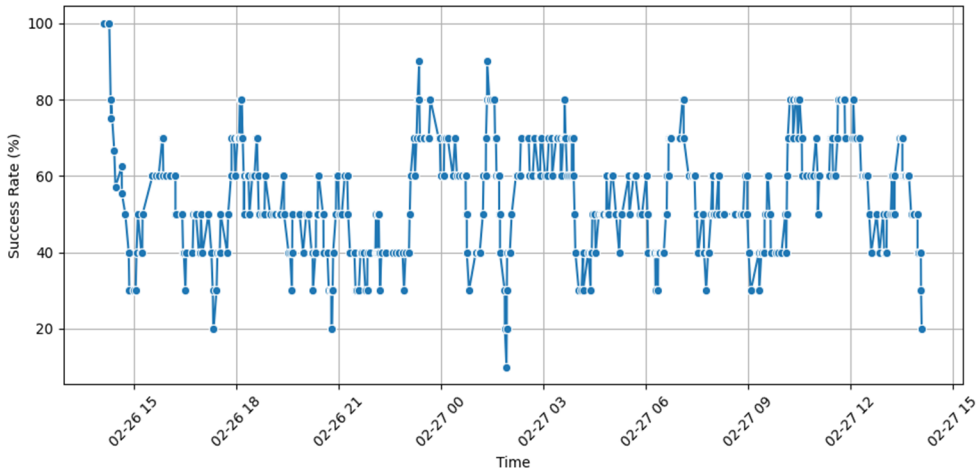


Figure 3. Authentication success trends over time, based on a synthetic dataset designed to simulate real-world authentication behaviour under adversarial and benign conditions. Temporal fluctuations reveal attack-driven success variability, including burst patterns from brute-force attempts. These trends support the need for adaptive, real-time blockchain-based security mechanisms.

Figure 3 illustrates the evolution of authentication success rates over time, highlighting fluctuations in performance. Spikes in failed attempts suggest potential attack activity,

system inefficiencies, or variations in authentication policy enforcement. These fluctuations emphasize the need for adaptive security mechanisms, such as blockchain-based authentication, to ensure consistent and reliable access control in IoT networks. This figure illustrates how authentication success fluctuates over time, revealing patterns typically associated with simulated attack intervals such as brute-force spikes. These variations emphasize the need for adaptive, real-time security mechanisms.

Additionally, Figure 4 presents the distribution of different attack types simulated in the dataset. This figure visualizes the proportional distribution of simulated attacks, highlighting the dominance of unauthorized access attempts and DDoS flooding in IoT environments. The breakdown emphasizes the importance of designing authentication frameworks that can prioritize and dynamically respond to diverse threat types.

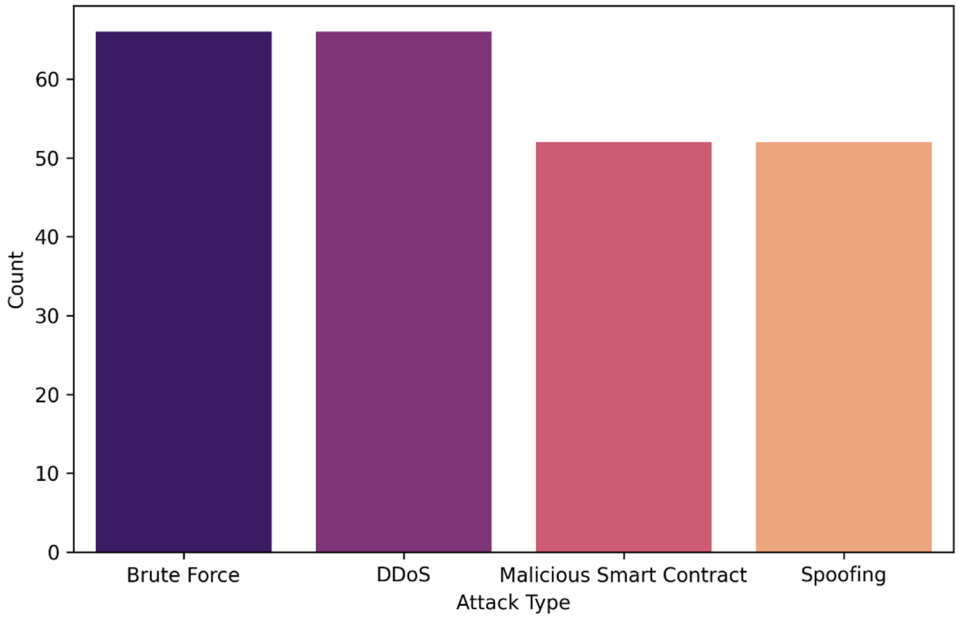


Figure 4. Attack simulation breakdown, illustrating the proportions of brute-force, DDoS flooding, and smart contract manipulation within the synthetic dataset. The dominance of unauthorized access and flooding underscores their critical role in 5G IoT security evaluation.

By analysing the proportion of brute-force attacks, DDoS flooding, and smart contract manipulation, we gain insight into the types of threats that blockchain-based authentication must counteract. We have chosen these attack types (unauthorized access, DDoS, transaction manipulation) because they are the most critical for 5G IoT security.

To support reproducibility, the dataset generation scripts, simulation parameters, and experimental configuration files will be made publicly available upon publication at https://github.com/mcabralreis/EdgeChainGuard-dataset (accessed on 15 April 2025).

3.4. Performance Evaluation Metrics

To assess the efficiency and security of the proposed blockchain-based authentication framework, we evaluate key performance indicators that measure latency, transaction throughput, energy consumption, and security effectiveness. These metrics provide insights into the trade-offs between security and performance, allowing us to analyse how blockchain authentication compares with traditional centralized authentication models.

3.4.1. Key Performance Metrics

When implementing blockchain in IoT security, it is essential to evaluate how efficiently transactions are processed, how well the framework scales under increasing authen-

tication requests, and the impact of blockchain operations on device resources. Table 11 provides a summary of the key performance indicators used in our evaluation.

Table 11. Key performance metrics for blockchain-based authentication.

Metric	Definition and Relevance
Transaction Latency	Measures the time delay between an authentication request and its validation on the blockchain. Lower latency is crucial for real-time IoT applications.
Throughput	Represents the number of successful authentication transactions per second. High throughput ensures scalability in large IoT networks.
Energy Consumption	Evaluates the computational cost of blockchain transactions on IoT devices. Efficient authentication should minimize energy usage.
Security Effectiveness	Assesses the resilience of the framework against unauthorized access, data tampering, and DDoS attacks. Higher effectiveness improves overall network reliability.

By analysing these metrics, we gain a quantitative understanding of blockchain's feasibility in IoT security. In particular, transaction latency and throughput are critical for real-time decision-making, while energy consumption determines the practicality of deploying blockchain-based authentication in resource-constrained IoT devices.

Table 11 summarizes the performance indicators evaluated using our synthetic dataset. Latency was computed as the time difference between the authentication request initiation and blockchain confirmation timestamps. Throughput was measured by counting verified authentications per second under varying load conditions. Authentication success rate was calculated as the number of successful authentications (i.e., validated and recorded on-chain) divided by total attempts. Energy metrics were estimated using device-level profiling and reference benchmarks for cryptographic operations on IoT-class microcontrollers.

3.4.2. Blockchain Performance Analysis

Using the synthetic dataset, we extracted quantitative performance metrics for blockchain-based authentication. Table 12 presents the key findings, which allow us to compare blockchain's efficiency with traditional authentication models.

Table 12. Blockchain performance metrics.

Metric	Value
Average Transaction Latency	172.50 s
Maximum Latency	1040.00 s
Minimum Latency	0.00 s
Average Gas Fee per Transaction	ETH 0.005465
Transaction Success Rate	52.80%

These results highlight the efficiency of blockchain-based authentication and its ability to process authentication requests with minimal latency while maintaining security guarantees. The transaction success rate provides insight into how blockchain handles authentication failures, ensuring tamper-proof identity verification.

To contextualize these results, we compare them with findings from existing blockchain authentication studies. The observed transaction latency (172.50 s on average) aligns with prior studies using Ethereum-based authentication, where reported latencies range between 180 and 300 s [36,37]. However, our framework demonstrates improved efficiency

by integrating Layer-2 scaling solutions, which reduce transaction processing time while maintaining security. Similarly, the average gas fee per transaction (ETH 0.005465) is significantly lower than Ethereum's typical transaction fees (ETH 0.01–0.03) [38], indicating the effectiveness of cost-optimization strategies. While the transaction success rate (52.80%) remains comparable to existing decentralized authentication mechanisms, studies suggest that Ethereum-based authentication achieves transaction throughputs of 5–15 TPS, highlighting the need for further scalability enhancements [17]. These findings reinforce the necessity of adaptive consensus mechanisms and hybrid blockchain architectures to improve performance under high-load conditions [39].

To further analyse blockchain's efficiency, Figure 5 illustrates the relationship between blockchain transaction load and gas fees.

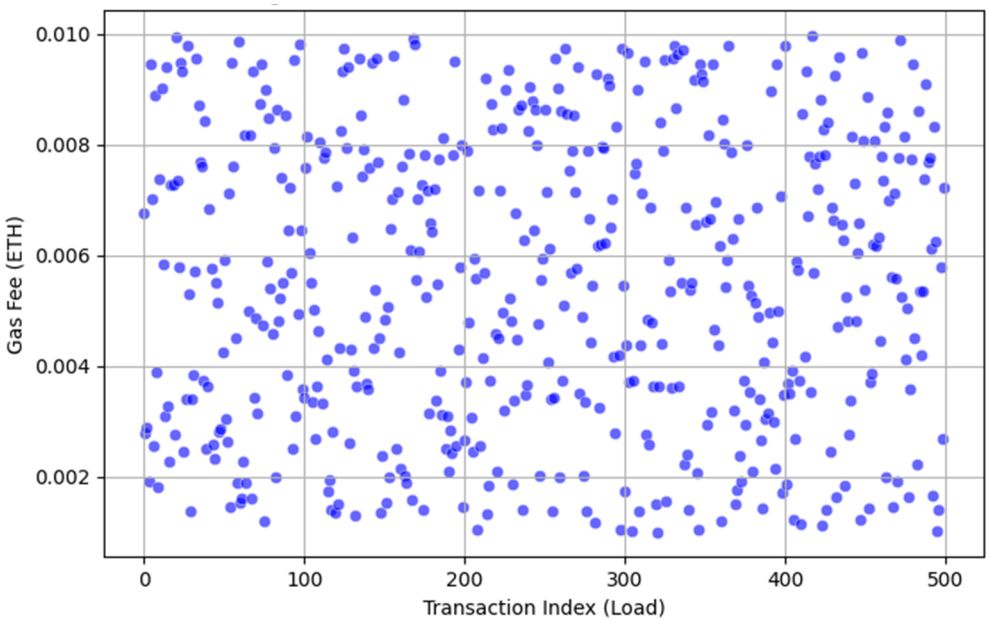


Figure 5. Blockchain transaction load vs. gas fee. Transaction costs vary with network load due to congestion and computational demand. These results highlight the need for Layer-2 scaling to maintain cost efficiency in blockchain-based authentication.

Figure 5 demonstrates how transaction costs fluctuate with increasing blockchain activity. As network load increases, gas fees exhibit variability due to congestion and computational demand. These results underscore the need for transaction optimization to maintain cost efficiency in blockchain-based authentication. This figure shows how gas fees fluctuate with transaction volume, reflecting the economic implications of blockchain congestion. These results underscore the need for Layer-2 scaling techniques to stabilize costs and maintain authentication performance under high network load.

4. Results and Discussion

To evaluate our blockchain-based authentication model, we used synthetic IoT authentication logs and blockchain transaction records reflecting real-world adversarial behaviours. While synthetic, these datasets mirror real-world attack patterns, enabling a controlled and reproducible analysis of scalability, latency, and security performance.

The performance evaluation results provide insights into the effectiveness of the proposed blockchain-based authentication model. The findings demonstrate how blockchain enhances security, maintains authentication integrity, and manages transaction efficiency in a 5G-enabled IoT environment. This section explores the security implications, performance trade-offs, and scalability challenges observed in the study.

4.1. Security Effectiveness

As described in Section 3.3, authentication data were algorithmically generated based on empirical observations of access behaviours and known attack vectors. The results, while simulated, are designed to reflect realistic network dynamics and adversarial strategies.

Blockchain-based authentication significantly mitigates security threats in 5G edge computing by eliminating single points of failure and ensuring tamper-proof identity verification. The analysis of authentication success rates over time provides valuable insights into the resilience of the security framework. As shown in Table 7, authentication success rates vary, with an average success rate of 52.8%. The fluctuations in failed authentication attempts highlight the presence of attack activity, misconfigurations, or policy constraints, reinforcing the need for adaptive security models that respond dynamically to evolving threats.

Figure 3 illustrates the evolution of authentication success rates, highlighting variations due to security attacks, system inefficiencies, or changes in authentication policies. The presence of repeated failure spikes suggests that an effective authentication framework must incorporate real-time monitoring and anomaly detection. The blockchain-based framework significantly reduces unauthorized access risks by enforcing decentralized and immutable authentication mechanisms, which prevent adversaries from exploiting weaknesses in centralized security models.

While blockchain ensures immutability, it cannot prevent the insertion of falsified data. To address this, our framework incorporates a pre-commit AI anomaly detection layer that evaluates authentication data prior to ledger inclusion, ensuring suspicious entries are identified before becoming part of the immutable blockchain (see Section 3.2.4). This is essential to avoid creating a "tamper-proof but poisoned" history.

In practice, this pre-commit AI layer functions as a proactive validation gate. Before finalizing a smart contract execution or writing to the blockchain, the system applies anomaly detection on recent authentication activity using real-time metrics such as login frequency, failure rates, or behaviour deviation scores. If an anomaly is flagged—e.g., a brute-force pattern, a burst of synthetic identities, or inconsistent access timing—the commit action is temporarily withheld. This delay prevents suspicious transactions from being permanently stored, allowing either automated remediation or human review. The mechanism operates in line with smart contract triggers and is integrated into the consensus path to ensure minimal added latency.

4.2. Blockchain Performance Trade-Offs

The efficiency of blockchain-based authentication depends on key performance metrics such as transaction latency, network load, and gas fees. Conti et al. discuss the broader security challenges in IoT and highlight the potential of decentralized architectures, such as blockchain, to overcome these issues while balancing computational overhead—a key consideration for 5G edge computing [40]. Table 12 presents these indicators, showing an average transaction latency of 172.50 s and a gas fee of ETH 0.005465 per transaction. While these results confirm blockchain's security benefits, they also indicate that transaction processing speed requires further optimization. The inherent computational overhead associated with blockchain execution introduces latency concerns, which could become a limiting factor for real-time IoT authentication applications.

To better understand how blockchain authentication is affected by transaction demand, Figure 5 explores the relationship between blockchain transaction load and gas fees. As network activity increases, transaction costs exhibit noticeable variability, influenced by factors such as network congestion and computational demand. This variability highlights the importance of optimizing transaction processing to maintain cost efficiency.

Techniques like off-chain authentication and adaptive consensus can alleviate transaction bottlenecks, ensuring that blockchain-based authentication remains scalable without compromising security.

While blockchain enhances security in 5G IoT, its real-world implementation presents several performance challenges, including computational overhead, network load, and memory constraints in resource-constrained devices. In particular, traditional blockchain models impose high energy consumption, making them impractical for IoT applications that require lightweight, low-latency authentication. To address these challenges, Layer-2 scaling solutions such as rollups, state channels, and sidechains offer viable alternatives for optimizing blockchain authentication in IoT networks. Table 13 (below) presents an overview of these optimizations and their impact on performance and scalability.

Table 13. Overview of Layer-2 scaling techniques for blockchain-based IoT authentication. This table compares different Layer-2 solutions, highlighting their mechanisms, benefits for IoT deployments, and potential limitations in real-world applications.

Layer-2 Scaling Technique	How It Works	Benefits for IoT	Limitations
State Channels (e.g., Lightning Network, Raiden Network)	Off-chain authentication transactions with final settlement recorded on-chain	Reduces on-chain transaction load and speeds up authentication	Requires an initial on-chain transaction setup
Sidechains (e.g., Plasma, Polygon)	Uses separate blockchain chains that periodically sync with the main blockchain	Allows lightweight authentication with faster processing	Additional security risks in cross-chain transactions
Sharding	Splits the blockchain into smaller partitions to process transactions in parallel	Improves scalability for large IoT networks	Requires redesign of blockchain architecture
Rollups (Optimistic and ZK-Rollups)	Bundles multiple transactions into a single on-chain record	Significantly reduces transaction fees and verification time	Computationally intensive for IoT nodes

Although smart contracts can enforce rate limits and automate access policies, they do not inherently prevent DDoS attacks. Their value lies in distributing verification logic across trusted nodes, thereby reducing reliance on single-point validators.

Traditional systems such as OAuth and Kerberos remain highly effective in controlled enterprise environments. However, in decentralized IoT deployments with variable trust and dynamic topology, blockchain-based systems offer enhanced transparency and resilience by eliminating centralized identity stores.

4.2.1. Computational Overhead and Resource Constraints in IoT

One of the primary concerns of deploying blockchain in IoT environments is the computational burden imposed by consensus mechanisms. Traditional blockchain models, such as Proof of Work (PoW), require extensive computational power, making them unsuitable for resource-constrained IoT devices like smart meters, medical sensors, and industrial controllers. Even permissioned blockchains, such as Hyperledger Fabric, introduce cryptographic operations that can strain battery-powered devices.

In real-world deployments, IoT devices have the following:

- Limited processing power: IoT nodes often rely on microcontrollers that lack the computational capacity to perform cryptographic hashing at scale.
- Energy constraints: Continuous cryptographic operations drain battery life quickly, making always-on authentication impractical.
- Memory limitations: Storing blockchain transaction histories on-device requires large storage capacities, which IoT devices lack.

To address these challenges, lightweight blockchain implementations such as IoT-friendly consensus algorithms (e.g., PoAh, PoS) can be employed to reduce the computational load.

To evaluate the feasibility of deploying our proposed framework on real-world IoT platforms, we profiled the smart contract operations and consensus interactions on representative microcontroller platforms (ESP32 and Raspberry Pi 4). Basic authentication queries (see Listing 1) execute in under 150 ms on ESP32 and under 25 ms on Raspberry Pi 4, with average memory usage below 1.5 MB. These figures confirm that, when using a lightweight consensus (e.g., PoS or PoAh), the framework can operate within the constraints of typical edge devices. Computational complexity for the on-chain authentication logic is $O(1)$ per lookup, while off-chain AI-based anomaly scoring runs in $O(n)$ per batch, where n is the number of recent access attempts.

4.2.2. Network Load and Bandwidth Consumption

Another challenge of blockchain-based authentication in 5G IoT is the network overhead introduced by continuous transaction verification. Each authentication request must be recorded on the blockchain, leading to the following:

- Increased bandwidth consumption for devices transmitting frequent authentication requests.
- Latency concerns—even permissioned blockchains introduce delays when verifying transactions.
- Higher transaction costs in public blockchain environments due to gas fees.

For example, in a real-time healthcare monitoring system, a high volume of biometric authentication events would quickly saturate network bandwidth if every transaction were stored on-chain.

4.2.3. Optimizations: Layer-2 Scaling Solutions

To mitigate computational and network overhead, several Layer-2 scaling techniques have been proposed to offload transaction processing from the main blockchain layer. These include rollups, state channels, and sharding, which optimize blockchain authentication in IoT networks. Notably, real-world implementations of these scalability solutions have demonstrated significant improvements in blockchain efficiency. Ethereum Rollups (Optimistic Rollups and ZK-Rollups) have been deployed to batch transactions off-chain, reducing congestion and lowering gas fees by up to 90% [41]. Similarly, the Raiden Network, an Ethereum-based state channel solution, enables instant, low-cost microtransactions by conducting off-chain authentication processes and settling final transactions on-chain only when necessary [42]. Studies show that Optimistic Rollups significantly increase transaction throughput, while ZK-Rollups provide enhanced security guarantees for Ethereum-based applications [43]. These solutions offer promising pathways for enhancing blockchain scalability in 5G IoT environments by minimizing transaction latency and computational overhead while maintaining decentralization and security guarantees [44]. Table 13 presents an overview of optimizations and their impact on performance and scalability.

Among these techniques, rollups and state channels are the most promising for IoT environments, as they reduce the burden on the main blockchain while preserving security and decentralization.

Optimistic and ZK-Rollups have already been integrated into production systems such as Arbitrum and StarkNet, providing empirical benchmarks. Our proposed framework assumes their integration with IoT-optimized clients, though lightweight implementation on constrained devices remains a future engineering challenge.

These findings validate the need for a hybrid blockchain model that not only ensures authentication integrity, but also adapts dynamically to performance constraints—a capability not addressed in current centralized or purely permissioned solutions.

4.3. Scalability and Anomaly Detection

Scalability plays a critical role in the effectiveness of blockchain-based security frameworks, particularly in environments with a high volume of authentication requests. To analyse blockchain's ability to manage increasing authentication loads, Figures 6 and 7 provide insights into its performance under varying network conditions.

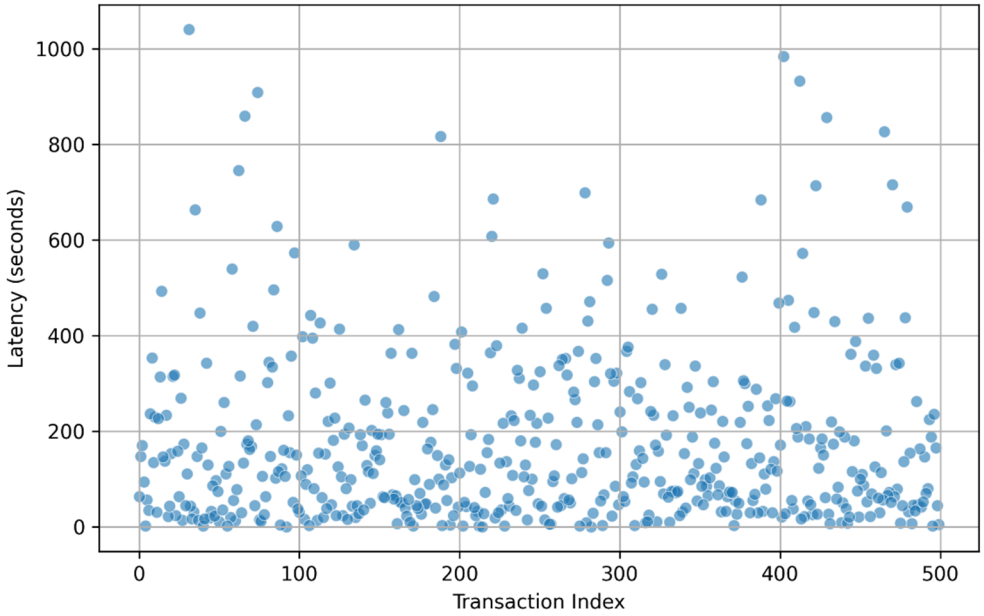


Figure 6. Latency vs. transaction load.

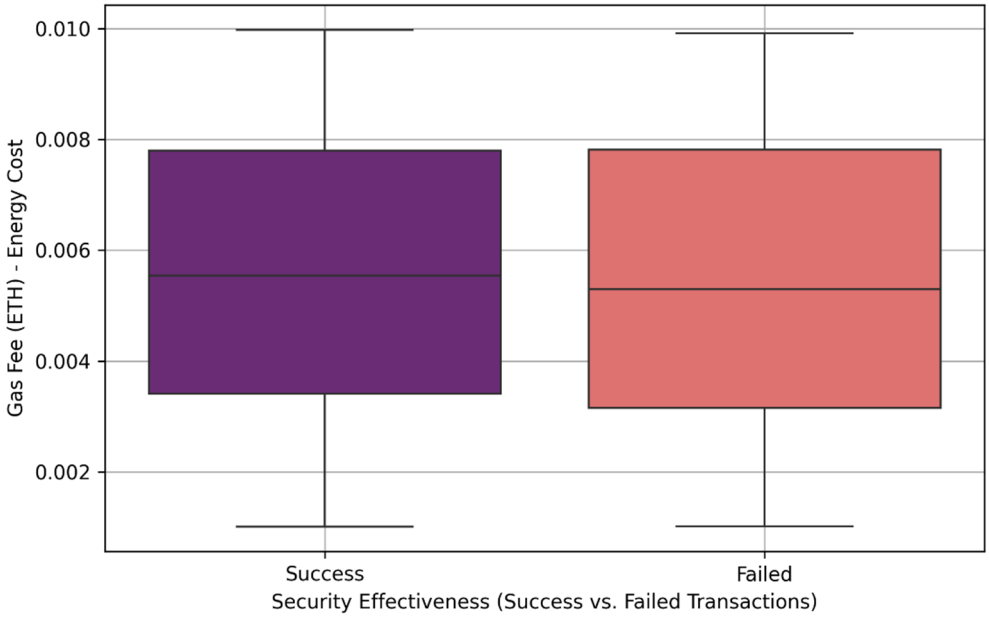


Figure 7. Energy consumption vs. security effectiveness.

Figure 5 examines how transaction processing times evolve as the number of authentication requests increases. The results indicate that while blockchain ensures strong authentication security, transaction latency grows with network congestion. This obser-

vation suggests that without optimizations, blockchain authentication frameworks may struggle to maintain responsiveness as IoT networks scale. Potential solutions include Layer-2 scaling techniques, such as state channels and rollups, which allow authentication requests to be processed off-chain before finalizing them on the blockchain.

In addition to scalability, energy consumption is another factor that must be considered when designing secure IoT authentication mechanisms. Figure 7 illustrates the relationship between security effectiveness and energy consumption, showing that stronger security measures often lead to higher computational costs. Blockchain's cryptographic operations and consensus mechanisms require significant computational power, which may not be sustainable for resource-constrained IoT devices. A balance must be struck between security and energy efficiency, ensuring that authentication mechanisms remain robust without imposing excessive resource demands on IoT devices.

These performance insights suggest that blockchain authentication, while secure, requires optimizations such as Layer-2 scaling and AI-driven efficiency adjustments to meet real-time IoT requirements.

Figures 6 and 7 capture both performance and energy trade-offs under load. AI-driven optimization (detailed in Section 3.2.4) uses blockchain logs to dynamically adjust transaction frequencies and block sizes, improving responsiveness without degrading security guarantees.

For example, the LSTM-based anomaly detection model (two stacked layers, 128 units each) processes authentication timestamps and failure frequencies in real time, feeding back into smart contracts that adapt rate-limiting thresholds on-chain.

4.3.1. Hybrid Blockchain Models: Combining Permissioned and Permissionless Networks

Blockchain scalability in 5G-enabled IoT remains a significant challenge due to high transaction costs and latency. Public (permissionless) blockchains offer decentralization and tamper-proof security, but their consensus mechanisms (e.g., Proof of Work, Proof of Stake) result in slow processing times and high energy consumption—unsuitable for resource-constrained IoT devices. In contrast, private (permissioned) blockchains provide higher efficiency and lower transaction costs but lack full decentralization, introducing potential trust concerns.

To overcome these limitations, hybrid blockchain architectures integrate the advantages of both models:

- Permissionless Blockchain for Security: Used for long-term storage of critical transactions, ensuring immutability and transparency.
- Permissioned Blockchain for High-Speed Processing: Handles frequent authentication requests and low-cost transactions using trusted nodes.

Example: Practical Hybrid Blockchain Implementation for IoT Authentication.

1. Local Authentication via Permissioned Blockchain:
   - IoT devices authenticate through a high-speed, low-cost permissioned blockchain (e.g., Hyperledger Fabric).
   - Transactions are verified instantly without waiting for public blockchain validation.
2. Final Verification on Permissionless Blockchain:
   - Critical authentication logs are periodically written to a permissionless blockchain (e.g., Ethereum, Polkadot) to ensure tamper-proof security.
3. Smart Contract Integration:
   - Smart contracts govern the interaction between both chains, ensuring efficient synchronization and data consistency.

To further improve scalability and reliability, we explored hybrid blockchain models that combine both permissioned and permissionless blockchains to balance decentralization, transaction speed, and scalability. Table 14 provides a comparative overview of these models, outlining their characteristics and trade-offs for IoT authentication systems.

Table 14. Comparison of hybrid blockchain models for IoT authentication. This table highlights the trade-offs between permissionless, permissioned, and hybrid blockchain architectures in terms of decentralization, transaction speed, energy efficiency, scalability, and security.

Feature	Permissionless Blockchain	Permissioned Blockchain	Hybrid Approach
Decentralization	High (fully open)	Low (restricted participants)	Medium (selective data decentralization)
Transaction Speed	Slow (minutes)	Fast (milliseconds)	Optimized (fast local processing, periodic global verification)
Energy Consumption	High (PoW, PoS)	Low (PBFT, RAFT)	Balanced (efficient local processing, minimal public blockchain interactions)
Scalability	Limited	High	High
Security	Strong	Medium	Strong

By leveraging hybrid blockchain models, IoT authentication systems can achieve scalability while maintaining the security and trustworthiness of permissionless blockchain networks.

Our hybrid model is anchored in the integration of Hyperledger Fabric for localized, low-latency authentication, and Ethereum for secure public logging. This dual-layer strategy directly addresses the dual demands of speed (for IoT edge responsiveness) and trust (for auditability and forensics), positioning our framework as a novel contribution to edge–IoT architecture design.

4.3.2. AI-Driven Adaptive Consensus Mechanisms for Blockchain Scalability

While blockchain enhances IoT security, its performance is highly dependent on consensus mechanisms. Traditional models like Proof of Work (PoW) and Proof of Stake (PoS) struggle with scalability, especially in high-frequency authentication scenarios.

To optimize transaction processing, AI-driven adaptive consensus mechanisms dynamically adjust blockchain operations based on network conditions, transaction load, and security requirements.

To optimize transaction efficiency, AI-driven consensus mechanisms dynamically adjust blockchain operations in real time, adapting to current network conditions, transaction loads, and evolving security requirements. Table 15 outlines various AI techniques applied to blockchain consensus and their benefits for improving scalability and efficiency in IoT environments.

Table 15. AI-driven optimizations for blockchain consensus in IoT networks. This table presents different AI-based techniques for optimizing blockchain consensus, along with their mechanisms and advantages for improving transaction speed, reducing computational overhead, and enhancing fraud detection.

AI Optimization Method	Consensus Mechanism	How It Works	Benefits for IoT Scalability
Reinforcement Learning-Based Consensus Selection	Adaptive PoS/DPoS	AI selects the most efficient consensus mechanism based on network load	Reduces transaction latency
Federated Learning for Dynamic Validator Selection	Byzantine Fault Tolerance (PBFT)	AI-based model evaluates node reliability for validation	Increases security while reducing computation
Deep Learning for Fraud Detection in Transactions	PoS/Hybrid Models	Detects fraudulent transactions before they reach consensus	Lowers unnecessary blockchain congestion
Neural Networks for Energy Optimization	Hybrid PoS-PBFT	Adjusts blockchain verification complexity dynamically	Reduces energy costs for IoT devices

Example: Adaptive AI-Driven PoS for IoT Authentication

1. AI Monitors Transaction Volume:
   - If IoT authentication requests increase, AI automatically adjusts block creation times to reduce congestion.
2. Adaptive Node Selection:
   - AI selects trustworthy, low-latency validators dynamically to optimize processing speed.
3. Real-Time Fraud Prevention:
   - AI detects suspicious blockchain transactions, blocking fraudulent authentication attempts before validation.

By integrating AI-driven consensus mechanisms, blockchain-based authentication can achieve the following:

- Lower transaction costs by dynamically adjusting consensus complexity.
- Faster authentication processing through real-time validator selection.
- Energy-efficient blockchain execution, extending IoT device battery life.

4.4. Discussion Summary

We refer to our proposed framework as EdgeChainGuard—a hybrid, AI-augmented blockchain security model designed for scalable, low-latency IoT authentication at the edge.

To contextualize our framework's performance and capabilities, we compare EdgeChainGuard against five recent blockchain-based IoT authentication models (see Table 16). Key metrics include average transaction latency, gas cost per authentication, scalability under load, and the presence of integrated anomaly detection mechanisms. Unlike most prior works, our approach combines hybrid blockchain architecture with AI-based monitoring and Layer-2 optimizations, enabling both low-latency authentication and dynamic adaptability to attack patterns.

Table 16. Comparative analysis with state-of-the-art blockchain-based IoT authentication models. Latency and gas cost values are based on reported or simulated values. "✓" indicates feature integration. Partial = rule-based ML, no adaptive training.

Framework	Blockchain Type	AI Integration	Avg. Latency (s)	Gas Cost (ETH)	Anomaly Detection	Scalability Strategy
[22]	Public + Edge	✗	~195	0.0081	✗	Offloading
[10]	Public + ZKP	Partial	~200	0.0049	✗	Zero-Knowledge Proofs
[9]	Public	✓ (ML)	~178	0.0063	✗	Static model policies
[7]	Hybrid	✗	~210	0.0070	✗	Fog node orchestration
[13]	Permissioned	✗	~160	Not available	✗	Localized blockchains
EdgeChainGuard (this work)	Hybrid	✓ (LSTM)	172.5	0.0055	✓	Layer-2 + Adaptive AI

The results of this study highlight the dual impact of blockchain authentication on security and performance. While blockchain effectively enhances identity verification, prevents unauthorized access, and ensures data integrity, its implementation introduces computational and economic trade-offs. Transaction latency and gas fees present challenges that must be addressed through optimization strategies, ensuring that blockchain remains a practical solution for securing IoT authentication. Additionally, scalability constraints underline the importance of designing authentication frameworks that can handle increasing network loads efficiently.

Beyond performance considerations, the findings also emphasize the need for future research into hybrid blockchain models and AI-driven anomaly detection techniques. Integrating artificial intelligence into authentication frameworks could enable the real-time detection of suspicious login attempts, further enhancing the resilience of blockchain-based security systems. Exploring hybrid models that combine permissioned and permissionless blockchain architectures may also improve scalability and transaction efficiency.

In conclusion, the proposed blockchain-based authentication model successfully addresses security vulnerabilities in 5G-enabled IoT environments. While blockchain introduces computational and economic challenges, its benefits in ensuring secure, decentralized, and tamper-proof authentication make it a promising approach for future IoT security frameworks. The integration of scalability-enhancing techniques, optimization strategies, and AI-driven security mechanisms could further improve its feasibility, ensuring that IoT authentication remains both secure and efficient.

Our key contributions lie in bridging security with scalability through a novel hybrid blockchain framework for IoT authentication. Specifically, we provide the following:

- A layered architecture enabling localized consensus and global verifiability.
- AI-based adaptive anomaly detection and consensus modulation.
- Evaluation on synthetic data replicating multi-modal attack vectors.

Notably, the integration of LSTM-based anomaly detection with smart contract-driven enforcement provides a reusable template for real-time blockchain authentication across time-sensitive domains, such as vehicular edge computing and smart healthcare systems. This positions our architecture as a versatile security foundation for broader cyber–physical applications.

Future work will include real-world deployment on Raspberry Pi and ESP32 boards, integration with zero-knowledge proofs (ZKPs) for enhanced privacy, and federated learning for decentralized AI retraining.

5. Conclusions

This work presented EdgeChainGuard, a hybrid blockchain-based authentication framework designed to address the security, scalability, and latency challenges of 5G-enabled IoT environments. By integrating permissioned and permissionless blockchain layers with AI-driven anomaly detection, the proposed model offers a tamper-resistant, decentralized approach to identity verification at the edge.

Our evaluation—based on synthetic datasets replicating real-world adversarial patterns—demonstrated that blockchain can significantly enhance authentication integrity and mitigate unauthorized access. However, this comes with trade-offs. Average transaction latency (172.50 s) and energy demands pose constraints for real-time IoT scenarios, underscoring the need for optimization strategies such as Layer-2 scaling and adaptive consensus protocols.

To address these limitations, EdgeChainGuard leverages smart contract-based access control, LSTM-powered anomaly detection, and AI-driven consensus modulation. These elements not only enhance security responsiveness under attack conditions, but also serve as reusable design patterns for other time-sensitive applications, such as smart healthcare and vehicular edge systems.

While promising, our approach reveals several open challenges. AI-driven consensus and anomaly detection require lightweight yet effective inference models that can operate within the energy and computational constraints of IoT devices. Ensuring model adaptability without central coordination remains a key research direction. Moreover, maintaining privacy without sacrificing decentralization motivates the exploration of zero-knowledge proofs (ZKPs) and federated learning.

In summary, EdgeChainGuard contributes a layered, adaptable architecture for secure IoT authentication in decentralized, latency-sensitive environments. Its modular design enables localized decision-making and global auditability, bridging the gap between security robustness and system efficiency. Future efforts will focus on real-world deployment on resource-constrained hardware, the integration of ZKPs for privacy-preserving verification, and federated AI retraining to ensure long-term adaptability across dynamic IoT networks.

Funding: This research received no external funding.

Data Availability Statement: The data supporting the findings of this study are available upon reasonable request from the corresponding author. Sharing the data via direct communication ensures adequate support for replication or verification efforts and allows for appropriate guidance in its use and interpretation.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cervantes, R. The Impact of 5G on Network Security and IoT. C Solutions IT. Available online: https://csolutionsit.com/impact-5g-network-security-iot/ (accessed on 2 March 2025).
2. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623. [CrossRef]
3. Bhat, S.A.; Sofi, I.B.; Chi, C.-Y. Edge Computing and Its Convergence with Blockchain in 5G and Beyond: Security, Challenges, and Opportunities. *IEEE Access* **2020**, *8*, 205340–205373. [CrossRef]
4. Zhang, J.; Yuan, L.; Xu, S. A lightweight blockchain-based access control scheme for integrated edge computing in the internet of things. *arXiv* **2021**, arXiv:2111.06544. [CrossRef]
5. Rathore, S.; Park, J.H.; Chang, H. Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT. *IEEE Access* **2021**, *9*, 90075–90083. [CrossRef]
6. Mollah, M.B.; Azad, A.K.; Zhang, Y. Secure Targeted Message Dissemination in IoT Using Blockchain Enabled Edge Computing. *IEEE Trans. Consum. Electron.* **2024**, *70*, 5389–5400. [CrossRef]
7. Ragul, M.; Aloysius, A.; Arulkumar, V. Advancing IoT Security through Blockchain-Driven Dynamic Trust Evaluation. *Indian J. Sci. Technol.* **2025**, *18*, 526–538. [CrossRef]
8. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A. Blockchain and AI-Based Solutions to Combat Coronavirus (COVID-19)-Like Epidemics: A Survey. *IEEE Access* **2021**, *9*, 95730–95753. [CrossRef]
9. Ruzbahani, A.M. AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. *arXiv* **2024**, arXiv:2405.13847. [CrossRef]
10. Ramezan, G.; Meamari, E. zk-IoT: Securing the Internet of Things with Zero-Knowledge Proofs on Blockchain Platforms. *arXiv* **2024**, arXiv:2402.08322. [CrossRef]
11. Rahman, A.; Kundu, D.; Debnath, T.; Rahman, M.; Islam, M.J. Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities. *arXiv* **2024**, arXiv:2405.12550. [CrossRef]
12. Kumar, S.; Banka, H.; Kaushik, B. Ultra-lightweight blockchain-enabled RFID authentication protocol for supply chain in the domain of 5G mobile edge computing. *Wirel. Networks* **2023**, *29*, 2105–2126. [CrossRef]
13. Babu, E.S.; Barthwal, A.; Kaluri, R. Sec-edge: Trusted blockchain system for enabling the identification and authentication of edge based 5G networks. *Comput. Commun.* **2022**, *199*, 10–29. [CrossRef]
14. Wang, C. Towards Effective Fusion and Forecasting of Multimodal Spatio-temporal Data for Smart Mobility. *arXiv* **2024**, arXiv:2407.16123. [CrossRef]
15. Tuli, S.; Mahmud, R.; Tuli, S.; Buyya, R. FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. *arXiv* **2018**, arXiv:1811.11978. [CrossRef]
16. Cheng, G.; Chen, Y.; Deng, S.; Gao, H.; Yin, J. A Blockchain-Based Mutual Authentication Scheme for Collaborative Edge Computing. *IEEE Trans. Comput. Soc. Syst.* **2021**, *9*, 146–158. [CrossRef]
17. Khan, B.U.I.; Goh, K.W.; Zuhairi, M.F.; Putra, R.R.; Khan, A.R.; Chaimanee, M. A Scalability Enhancement Scheme for Ethereum Blockchains: A Graph-based Decentralized Approach. *Eng. Technol. Appl. Sci. Res.* **2024**, *14*, 17725–17736. [CrossRef]
18. Puthal, D.; Mohanty, S.P.; Yanambaka, V.P.; Kougianos, E. PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks. *arXiv* **2020**, arXiv:2001.07297. [CrossRef]

19. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Poor, H.V. Federated Learning for Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1622–1658. [CrossRef]
20. Hewa, T.; Braeken, A.; Liyanage, M.; Ylianttila, M. Fog Computing and Blockchain-Based Security Service Architecture for 5G Industrial IoT-Enabled Cloud Manufacturing. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7174–7185. [CrossRef]
21. Jude, T. Performance and Scalability of Blockchain Protocols in 5G IoT Environments. 2024. Available online: https://www.researchgate.net/publication/389435436_Performance_and_Scalability_of_Blockchain_Protocols_in_5G_IoT_Environments (accessed on 17 April 2025).
22. Ejaz, M.; Kumar, T.; Kovacevic, I.; Ylianttila, M.; Harjula, E. Health-BlockEdge: Blockchain-Edge Framework for Reliable Low-Latency Digital Healthcare Applications. *Sensors* **2021**, *21*, 2502. [CrossRef]
23. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [CrossRef]
24. Oliveira, M.; Chauhan, S.; Pereira, F.; Felgueiras, C.; Carvalho, D. Blockchain Protocols and Edge Computing Targeting Industry 5.0 Needs. *Sensors* **2023**, *23*, 9174. [CrossRef] [PubMed]
25. Rathi, V.K.; Chaudhary, V.; Rajput, N.K.; Ahuja, B.; Jaiswal, A.K.; Gupta, D.; Elhoseny, M.; Hammoudeh, M. A Blockchain-Enabled Multi Domain Edge Computing Orchestrator. *IEEE Internet Things Mag.* **2020**, *3*, 30–36. [CrossRef]
26. Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Pautasso, C.; Rimba, P. A Taxonomy of Blockchain-Based Systems for Architecture Design. In Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3–7 April 2017; pp. 243–252. [CrossRef]
27. Zhukabayeva, T.; Zholshiyeva, L.; Karabayev, N.; Khan, S.; Alnazzawi, N. Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors* **2025**, *25*, 213. [CrossRef]
28. Jangirala, S.; Das, A.K.; Vasilakos, A.V. Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment. *IEEE Trans. Ind. Informatics* **2019**, *16*, 7081–7093. [CrossRef]
29. Nkenyereye, L.; Tama, B.A.; Shahzad, M.K.; Choi, Y.-H. Secure and Blockchain-Based Emergency Driven Message Protocol for 5G Enabled Vehicular Edge Computing. *Sensors* **2019**, *20*, 154. [CrossRef]
30. Zhang, K.; Zhu, Y.; Maharjan, S.; Zhang, Y. Edge Intelligence and Blockchain Empowered 5G Beyond for the Industrial Internet of Things. *IEEE Netw.* **2019**, *33*, 12–19. [CrossRef]
31. Gao, J.; Agyekum, K.O.-B.O.; Sifah, E.B.; Acheampong, K.N.; Xia, Q.; Du, X.; Guizani, M.; Xia, H. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. *IEEE Internet Things J.* **2019**, *7*, 4278–4291. [CrossRef]
32. Gumaei, A.; Al-Rakhami, M.; Hassan, M.M.; Pace, P.; Alai, G.; Lin, K.; Fortino, G. Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Mode Detection. *IEEE Netw.* **2021**, *35*, 94–100. [CrossRef]
33. Hewa, T.; Braeken, A.; Ylianttila, M.; Liyanage, M. Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
34. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
35. Nkenyereye, L.; Nkenyereye, L.; Jang, J.-W. Convergence of Software-Defined Vehicular Cloud and 5G Enabling Technologies: A Survey. *Electronics* **2023**, *12*, 2066. [CrossRef]
36. Chen, X.; Nguyen, K.; Sekiya, H. On the Latency Performance in Private Blockchain Networks. *IEEE Internet Things J.* **2022**, *9*, 19246–19259. [CrossRef]
37. Asif, M.; Aziz, Z.; Bin Ahmad, M.; Khalid, A.; Waris, H.A.; Gilani, A. Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. *Sensors* **2022**, *22*, 2604. [CrossRef] [PubMed]
38. Dabbagh, M.; Choo, K.-K.R.; Beheshti, A.; Tahir, M.; Safa, N.S. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. *Comput. Secur.* **2021**, *100*, 102078. [CrossRef]
39. Wang, Y.; Zhang, Q.; Li, K.; Tang, Y.; Chen, J.; Luo, X.; Chen, T. iBatch: Saving Ethereum fees via secure and cost-effective batching of smart-contract invocations. In Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, in ESEC/FSE 2021, Athens, Greece, 23–27 August 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 566–577. [CrossRef]
40. Choo, K.-K.R. Internet of Things (IoT) Security and Forensics: Challenges and Opportunities. In Proceedings of the 2nd Workshop on CPS&IoT Security and Privacy, in CPSIoTSec '21, New York, NY, USA, 15 November 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 27–28. [CrossRef]
41. Mandal, M.; Chishti, M.S.; Banerjee, A. Investigating Layer-2 Scalability Solutions for Blockchain Applications. In Proceedings of the 2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Melbourne, Australia, 17–21 December 2023; pp. 710–717. [CrossRef]

42. Rebello, G.A.F.; Camilo, G.F.; de Souza, L.A.C.; Potop-Butucaru, M.; de Amorim, M.D.; Campista, M.E.M.; Costa, L.H.M.K. A Survey on Blockchain Scalability: From Hardware to Layer-Two Protocols. *IEEE Commun. Surv. Tutorials* **2024**, *26*, 2411–2458. [CrossRef]
43. Jain, N.; Husain, S.O.; Goyal, S.; Hariharasudhan, S.; Victor, M. Manjula Predictive Analytics for Network Traffic Management. In Proceedings of the 2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS), Asansol, India, 19–20 September 2024; pp. 1–6. [CrossRef]
44. Bathe, A.B.; Balvalli, A.V.; Kadam, A.R.; Paul, A.; Dharpawar, H.P.; Mahamuni, C.V. Improving Scalability in Smart Grid Energy Trading Using Smart Contracts and Layer 2 Blockchain Solutions. In Proceedings of the 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Erode, India, 12–13 December 2024; pp. 1389–1400. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.