TL2AB : Trusted lightweight authentication using AI and blockchain for 6G networks

TL2AB : Trusted Lightweight Authentication using AI and Blockchain for 6G Networks

Sabrina Sakraoui[a], Makhlouf Derdour[b], Ahmed Ahmim[c], Reham Almukhlifi[d], Marwa Ahmim[a], Insaf Ullah[e]

[a] *Networks and Systems Laboratory, Department of Computer Science,Badji Mokhtar Annaba University, Department and Organization addressline Annaba, 23000, , Algeria*
[b] *Department of omputer Science, Oum El Bouaghi University, Department and Organization addressline Oum El Bouaghi, 4000, , Algeria*
[c] *Department of Computer Science, Mohamed-Cherif Messaadia University, Department and Organization addressline Souk Ahras, 41000, , Algeria*
[d] *Cybersecurity Department ,College of Computer Science and Engineering, Taibah University, Department and Organization addressline Medina, 42353, , Saudi Arabia*
[e] *Institute for Analytics and Data Science, University of Essex, Department and Organization addressline Essex, CO43SQ, , United Kingdom*

Abstract

The upcoming era of Sixth-Generation technology brings about special opportunities and challenges with respect to cybersecurity, especially regarding secure authentication mechanisms. This paper introduces TL2AB, a trusted lightweight authentication framework using artificial intelligence and blockchain technology. The proposed solution addresses critical security and privacy issues related to 6G applications, particularly in sensitive sectors such as healthcare and IoT. TL2AB enhances security in communication by introducing a new three-factor authentication scheme while allowing users to access rapidly and efficiently. TL2AB not only meets the high demands of 6G networks but also creates a robust foundation for future research in secure authentication frameworks.

Keywords: Security, Privacy, Authentication, Blockchain, 6G, Anomaly Detection.

1. Introduction

The world is moving into one of the fastest-evolving times, from 5G to 6G networks in wireless communications [1]. Compared to its predecessor, 6G is envisioned to offer unrivaled connectivity through ultra-low latency and support massive IoT ecosystems that make transformative applications such as smart cities, autonomous systems, and even next-generation AR and VR possible [2]. Still, new security concerns come with new advancements. While this trend is coupled with enhanced network complexity, the risks for cyber-attacks increase dramatically, including data breaches and privacy violations [3]. In this respect, lightweight and scalable authentication mechanisms that are capable of securing communication within highly dynamic and resource-constrained environments have to be developed to enhance trustworthiness and security.

Most of the existing authentication protocols, which were designed mainly for both 4G and 5G [4], cannot meet strict performance and security requirements for 6G [5]. They are either too resource-intensive to operate on the small, low-power devices pervasive in IoT, or too rigid to be adaptive to the dynamic nature of 6G wireless networks that require real-time decision-making and context-awareness. Besides, the centralized nature of most current security architectures creates bottlenecks and single points of failure, which are vulnerable to attacks.

In this paper, we propose TL2AB, a novel authentication framework that merges blockchain with the power of Artificial Intelligence (AI) to ensure robustness, lightweight, and decentralized security for 6G networks. TL2AB leverages the immutability provided by blockchain and its distributed trust model in developing a decentralized and tamper-proof authentication architecture. Meanwhile, AI-powered continuous authentication is monitoring the behavior of that device in real time-reacting to the emerging threats. The decentralized nature of blockchain, combined with the adaptive learning functions of AI, powers TL2AB with the following key advantages:

- *Lightweight Architecture:* computation-friendly lightweight architecture is designed to work in perfect harmony with resource-constrained IoT devices, constituting the major component of the 6G ecosystem.

- *Decentralized Trust:* The blockchain removes a single point of failure, hence enhancing security, scalability, and resilience against cyberattacks.

- *AI-powered Adaptive Security:* The AI continuously monitors for threats and updates the risk assessment in real time to make changes to security protocols without added overhead.

- *Scalability:* Such architecture would scale with the enormous size of 6G toward relentless authentication of billions of interconnecting devices.

This paper introduces the TL2AB architecture, elucidating in detail its components and interplay among AI, blockchain, and 6G edge nodes. The proposed framework targets the support of not only device-to-network communication but also device-to-device authentication, crucial in such a decentralized environment as is 6G. We will go through the mathematical model, the consensus mechanism, and the continuous AI-based risk profiling driving the dynamic nature of authentication.

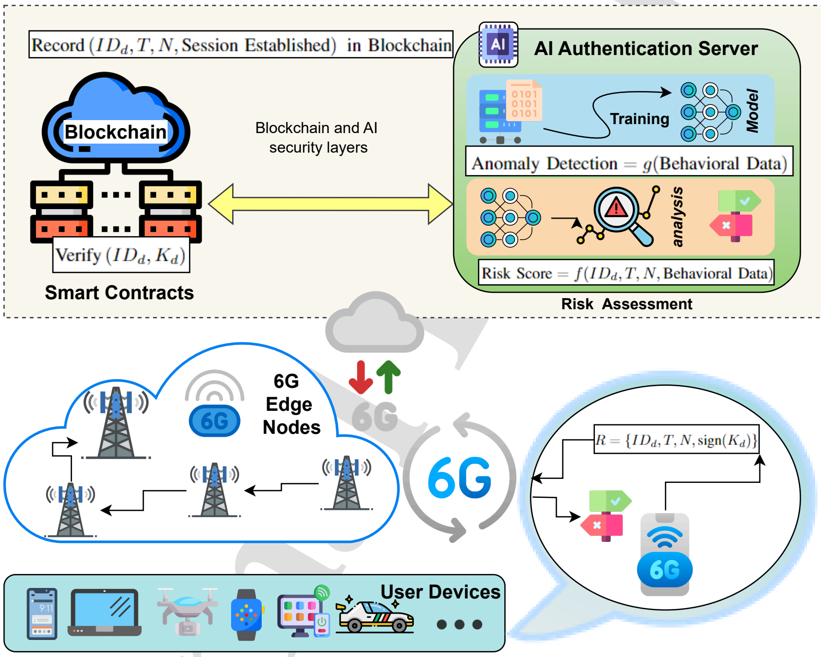

Record $(ID_d, T, N, \text{Session Established})$ in Blockchain
AI
AI Authentication Server
0101 0101 0101
Training
Model
Anomaly Detection $= g(\text{Behavioral Data})$
Blockchain
Blockchain and AI security layers
analysis
Verify (ID_d, K_d)
Smart Contracts
Risk Score $= f(ID_d, T, N, \text{Behavioral Data})$
Risk Assessment
6G
6G Edge Nodes
6G
6G
$R = \{ID_d, T, N, \text{sign}(K_d)\}$
6G
User Devices

Figure 1: TL2AB architecture

2. Related Works

Transitions to 6G technology have attracted a significant amount of research into enhancing security and authentication mechanisms in the direction of wide-scale applications, including: healthcare, sea transportation, satellite networks, and blockchain-based systems [6, 7, 8]. The section below undertakes a review of a selected related literature on the security challenges pertaining to 6G networks and different proposed solutions, as provided in Tab. 1.

Paper	**Application Domain**	**Security Mechanism**	**Authentication Approach**	**Technological Focus**
Le et al. [6]	Healthcare	Data Privacy, System Cost Optimization	Three-factor authentication (Smart Card, Password, Biometric)	Healthcare Networks, Authentication Protocols
Chaudhry et al. [8]	Maritime Transportation Systems	GPS Spoofing, Unauthorized Data Access	Lightweight Authentication Protocol	Maritime Security, GPS-based Systems
Tao et al. [7]	Satellite Networks	Privacy Preservation, Energy Efficiency	Bilinear Pairing-based Group Signature, Batch Authentication	Satellite-ground Integrated Networks
Asim et al. [9]	Blockchain	Multi-Factor Authentication (MFA), Cyber Attack Prevention	MFA in Blockchain Systems	Blockchain-based Security, Cybersecurity
Fang et al. [10]	IoT Networks	Security Management, Authentication Efficiency	AI-enabled Lightweight Authentication, Holistic Access Control	IoT Networks, AI-enhanced Security
Garabato et al. [11]	General (Authentication Systems)	Continuous Authentication, Activity Monitoring	AI-based Continuous Authentication (SVM, MLP, Deep Learning)	AI-driven Authentication, Continuous User Verification

Table 1: Summary of Related Works on Security and Authentication in 6G Networks

The authors in [6] proposed CL-UCSSO, which is an authentication protocol based on a three-factor authentication mechanism involving a smart card, password, and biometric authentication. Further, it allows network communication between patients and healthcare providers efficiently. Accordingly, it addresses issues and challenges over data privacy and system cost. The proposed protocol has been tested with well-known verification tools, proving its superior performance and features compared to existing protocols. Another work in [8] investigated the security and privacy vulnerabilities in 6G-enabled Maritime Transportation Systems. The authors therein propose a lightweight authentication protocol to provide protection against security threats by GPS spoofing and unauthorized data access. The formal methods of security assessment allow the authors to prove that their protocol provides enhanced features of security compared to traditional authentication schemes. This research emphasizes the need for adaptable security mechanisms tailored to each particular sector of the 6G ecosystem. The paper in [7] introduced an authentication protocol for preserving privacy in a heterogeneous satellite-ground integrated network. The authors introduce a bilinear pairing-based short group signature algorithm that shall offer unlinkable authentication and a lightweight batch authentication protocol of low-energy nodes, which is resistant to DoS attacks with efficiency. Their work also illustrates one of the challenges when roaming across different operator networks and the needed implementations toward efficient cross-domain authentication protocols, reducing latency. The work in [9] presented a review of security issues in 6G networks, depicts high expectations regarding the use of blockchain technology to increase both security and authentication. The paper also articulates the use of MFA techniques within a blockchain system to prevent different types of sophisticated cyberattacks. This work depicts that addressing particular vulnerabilities associated with applications is in demand, and blockchain is probably going to be one of the most promising solutions for upcoming security demands.

Besides improving security in such environments with the leverage of AI, two other solutions are developed that can be enabled by AI: a lightweight authentication scheme and a holistic access control scheme. The most important conclusion was that AI can make security management simpler and might adapt to the dynamic ecosystem of IoT, pointing out some future research directions such as cooperative access control, advanced machine learning algorithms, and game theory-based defense mechanisms.

Various existing studies have explored applying AI techniques to improve authentication and authorization in large-scale IoT networks. One introduced the characteristics of IoT networks and the challenges with conventional authentication approaches [10]. By identifying the advantages of using AI to improve security in these environments, the authors went on to propose two new AI-enabled solutions: a lightweight authentication scheme and a holistic access control scheme. The important conclusion derived was that AI could make security management simpler and would adapt to the dynamic IoT ecosystem. It also drew on future research directions, including cooperative access control, advanced machine learning algorithms, and game theory for defense mechanisms. Another work analyzed the feasibility of AI-based continuous authentication in [11]. The authors prepared a custom application to gather user activity data in a guided scenario and also used a public dataset for benchmarking in a non-guided setting. They developed key features from that data and trained three different AI models: Support Vector Machines, Multi-Layer Perceptrons, and a Deep Learning approach. These indeed proved to be effective AI-powered techniques for user verification across both guided and non-guided environments. Then, they developed a system for continuous authentication using weighted sliding windows to detect impostor sessions in real-world situations.

In the past few years, various lightweight authentication protocols have been proposed for IoT networks, most of which employed advanced technologies like blockchain, implicit certificates, PUFs, and AI-based systems. For example, Siddhartha et al. [12] proposed an implicit certificate-based three-factor authentication protocol for IoT applications in the healthcare industry that provides robust multi-factor security at the expense of high computation overheads and poor scalability. Similarly, Vipin Kumar et al. [13] designed a light authentication protocol for IoT devices used in a smart home that effectively resists replay, spoofing, and man-in-the-middle attacks.

Khalid et al. [14] proposed a decentralized blockchain-based authentication scheme for IoT networks, leveraging the inherent distributed trust of blockchain for safe key management but at the cost of very high processing overhead. Al Ahmed et al. [15] proposed a blockchain-inspired Authentication-Chains protocol that uses cluster-based authentication with a novel consensus algorithm with low computational overhead, but suffers from heterogeneous network integration. In addition, Aman et al. [16] presented a PUF-based mutual authentication scheme designed for resource-constrained IoT devices that is extremely secure against side-channel and physical attacks. Lastly, Tahir et al. [17] proposed a blockchain-enabled authentication and authorization protocol for IoT networks for health informatics, which provides high mutual authenticity and access control while reducing the communication and computation overhead.

For a general comparison, Tab. 2 summarizes the key security features, authentication techniques, technical focus, and limitations of the cited works and our TL2AB proposal. As can be seen from the comparison, the limitations of the existing solutions – i.e., scalability problems, computational costliness, or lack of complete continuous monitoring – are what TL2AB aims to address by the integration of decentralized blockchain-based trust with AI-driven dynamic risk assessment for 6G networks.

Table 2: Comparison of Security Features and Authentication Approaches in Related Schemes

Reference	**App. Domain**	**Security Mechanism**	**Authentication Approach**	**Tech. Focus**	**Key Security Features and Limitations**
[12]	Healthcare IoT	Implicit Certificate-based	Three-factor (Smart Card, Password, Biometric)	6G Healthcare	Robust multi-factor security; high computational cost and limited scalability.
[13]	Smart Home IoT	Implicit Certificate-based	Lightweight Device-to-Device Authentication	Smart Home IoT	Optimized for resource-constrained devices; resists replay and MITM attacks.
[14]	General IoT Systems	Blockchain-based	Decentralized Authentication	IoT Networks	Leverages decentralized trust; may incur processing overhead.
[15]	IoT Networks	Blockchain-inspired	Cluster-based Authentication with Consensus	IoT Networks	Novel consensus algorithm with low computational overhead; challenges with heterogeneous integration.
[16]	IoT Systems	PUF-based	Lightweight Mutual Authentication	IoT	High efficiency and robust resilience against physical and side-channel attacks; tailored for constrained environments.
[17]	Health Informatics	Blockchain-enabled	Probabilistic Authentication and Authorization	Healthcare IoT	Robust mutual authentication with enhanced access control and lower overhead; designed specifically for health informatics.
TL2AB (Proposed)	**6G Networks, IoT**	**AI-driven Continuous Authentication with Blockchain**	**Dynamic, Adaptive Multi-factor Authentication**	**6G, IoT**	**Integrates decentralized trust with AI-driven risk assessment for real-time, scalable, and resource-efficient authentication; introduces continuous monitoring and dynamic adaptation to emerging threats.**

Variable	**Description**
ID_d	A unique identifier assigned to each device in the network.
K_d	The cryptographic key generated for each device, used to sign authentication requests and secure communications.
R	The authentication request message, which includes ID_d, T, N, and $sign(K_d)$.
T	The timestamp indicating when the authentication request is generated; used to prevent replay attacks.
N	A unique nonce included in each authentication request to ensure its uniqueness and counter replay attacks.
$sign(K_d)$	The digital signature produced using the device's key K_d, ensuring the authenticity and integrity of the request.
RS	The risk score computed by the AI Authentication Server, normalized between 0 and 1 to reflect the likelihood of a security threat.
$T_{\text{threshold}}$	The predefined risk score threshold above which additional authentication measures are required.
$P(\text{MITM})$	The estimated probability of a successful Man-in-the-Middle attack on the system.
$P(\text{Impersonation})$	The estimated probability of a successful impersonation attack on the system.
$P(\text{DoSTL2AB})$	The estimated probability of a successful Denial-of-Service attack against the TL2AB framework.
$P(\text{DoScentralized})$	The estimated probability of a successful Denial-of-Service attack against a centralized authentication system, provided for comparison.
$P(E)$	The estimated probability of a privacy breach event occurring within the system.

Table 3: Symbols Definition

3. System and Network Model

This section presents the architecture and operational steps of TL2AB, as illustrated in Fig. 1. The proposed framework integrates blockchain technology and AI to create a secure, efficient, and adaptive authentication mechanism suitable for 6G networks.

3.1. TL2AB Architecture

The architecture of TL2AB includes a few important components put to operate in conjunction, enabling secure authentication in 6G environments:

3.1.1. User Devices

In other words, IoT devices, mobile phones, and sensors will be required to get authentication before connecting to the network. Each user device should have a unique cryptographic key at a secure element of the device.

3.1.2. 6G Edge Nodes

These are interfaces between the user devices and the rest of the network. They work like middle entities between the device and the remaining network, forwarding authentication requests as well as responses.

3.1.3. AI Authentication Server

This is an intelligent server driven by AI through machine learning algorithms. It analyzes the authentication requests from the user-side device and the behavioral pattern to generate a verdict on the device's risk. It adjusts its authentication requirements based on real-time threats.

3.1.4. Blockchain Network

The decentralized blockchain serves as the spine for the TL2AB Authentication Framework. The network provides trust with immutability, hence storing all authentication requests and their outcomes. Thus, it further carries the properties of transparency and traceability.

3.1.5. Smart Contracts

Smart contracts deployed on the blockchain, automate this authentication process by defining a set of rules or criteria for successful authentication. They ensure that the terms of service are met before access is granted.

3.2. System Assumptions

The key assumptions underlying the TL2AB framework are as follows:

- The underlying blockchain network is secure against 51% attacks and other consensus-related vulnerabilities, considering the fact that a majority of nodes comprising it are honest.

- In the user's devices, use a secure element that securely store the unique cryptographic keys used by users without compromising security.

- The AI Authentication Server can collect enough behavioral data to model the activities of users with high accuracy and also spot anomalies.

- There might be some adversaries that can intercept and manipulate the messages of communication and might compromise individual devices or nodes in the network.

- The AI models are trained using clean data that has not been compromised in any way, making them quite reliable in the risk assessment process.

Algorithm 1 TL2AB Authentication Algorithm (Part 1)

```
procedure RegisterDevice($ID_d, K_d$)
    Generate cryptographic key $K_d$ and store $(ID_d, K_d)$ in Blockchain.
    return ”Device Registered”
end procedure
procedure AuthenticationRequest($ID_d, K_d$)
    Generate timestamp $T$ and nonce $N$.
    $R \leftarrow \{ID_d, T, N, \text{Sign}(K_d)\}$
    return $R$
end procedure
procedure AssessRisk($R$)
    Analyze behavioral data associated with $ID_d$.
    $RS \leftarrow f(ID_d, T, N, \text{BehavioralData})$
    return $RS$
end procedure
procedure ExecuteSmartContract($R$)
    if Verify($ID_d, K_d$) in Blockchain then
        Record authentication attempt in Blockchain.
        return ”Authentication Successful”
    else
        return ”Authentication Failed”
    end if
end procedure
```

Algorithm 2 TL2AB Authentication Algorithm (Part 2)

```
procedure AdjustAuthentication($RS$)
    if $RS > T_{\text{threshold}}$ then
        Require additional factors (Biometric, OTP).
        if additional factors are provided then
            return "Authentication Successful"
        else
            return "Authentication Failed"
        end if
    else
        return "Authentication Successful"
    end if
end procedure
procedure EstablishSession($ID_d$)
    Encrypt Data and record session in Blockchain.
    return "Session Established"
end procedure
procedure MonitorSession($ID_d$)
    while session is active do
        Check for anomalies in behavioral data.
        if AnomalyDetected() then
            TerminateSession($ID_d$) and require re-authentication.
        end if
    end while
end procedure
procedure TerminateSession($ID_d$)
    Record session termination in Blockchain.
    return "Session Terminated"
end procedure
procedure Main
    // Register Device
    RegisterDevice($ID_d, H(K_d)$)
    // Authentication Process
    $R \leftarrow$ AuthenticationRequest($ID_d, KH(K_d)$)
    $RS \leftarrow$ AssessRisk($R$)
    if $RS < T_{\text{threshold}}$ then
        if ExecuteSmartContract($R$) == "Authentication Successful" then
            AdjustAuthentication($RS$)
            EstablishSession($ID_d$)
            MonitorSession($ID_d$)
        else
            return "Authentication Failed"
        end if
    else
        Require additional authentication.
    end if
end procedure
```

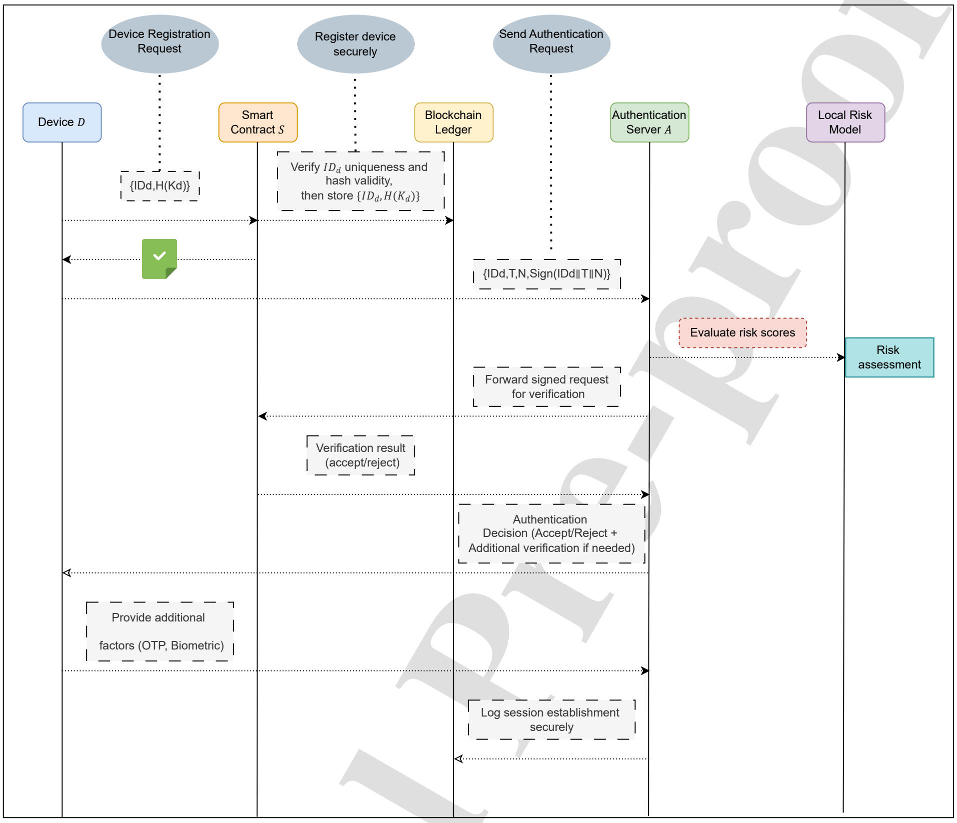

Device Registration Request
Register device securely
Send Authentication Request
Device D
Smart Contract S
Blockchain Ledger
Authentication Server A
Local Risk Model
{IDd,H(Kd)}
Verify ID_d uniqueness and hash validity, then store $\{ID_d, H(K_d)\}$
{IDd,T,N,Sign(IDd‖T‖N)}
Evaluate risk scores
Risk assessment
Forward signed request for verification
Verification result (accept/reject)
Authentication Decision (Accept/Reject + Additional verification if needed)
Provide additional factors (OTP, Biometric)
Log session establishment securely

Figure 2: Execution Flowchart of the TL2AB Authentication Protocol

3.3. Operational Steps of TL2AB

The TL2AB authentication process consists of a sequential order of operations designed to offer secure, efficient, and adaptive authentication. The architecture integrates blockchain-based identity authentication, AI-based risk assessment, and dynamic multi-factor authentication (MFA) to provide robust security while guaranteeing usability. The complete execution process of the TL2AB authentication protocol is illustrated in Fig. 2. It summarizes the key messages exchanged and the interactions between the device, the authentication server, the smart contract, and the blockchain ledger. The following steps outline the entire authentication process.

3.3.1. Step 1: Registration

A smart contract deployed on the blockchain handles the verification of this request. The verification procedure includes:

- **Uniqueness check:** The smart contract ensures that the identifier ID_d is not already registered by querying the ledger state.
- **Hash format validation:** The format and length of $H(K_d)$ are validated against expected parameters (e.g., 256-bit SHA-256 output).
- **Replay protection:** A nonce or timestamp is included in the transaction to protect against replay attacks.
- **Authenticity assurance (optional):** If needed, an off-chain verifier (e.g., PKI server or TEE attestation service) may confirm that K_d was generated inside a trusted module and is tied to the device ID_d.

If all checks pass, the pair $\{ID_d, H(K_d)\}$ is recorded immutably on the blockchain, enabling only registered devices to initiate authentication requests in future sessions.

The formal notation of the registration operation is:

$$\text{RegisterDevice}(ID_d, H(K_d)) \Rightarrow \text{Blockchain Entry}$$

3.3.2. Authentication Request Generation

When a device attempts to authenticate, it generates an authentication request containing its identity ID_d, a timestamp T, and a nonce N. To ensure integrity and authenticity, the device signs a specific set of values using its private key K_d stored in the TEE.

The digital signature is computed over the concatenation of the request components as follows:

$$\text{Sign}(K_d, M) \quad \text{where } M = \{ID_d \parallel T \parallel N\}$$

This signature proves the origin and integrity of the message without revealing K_d. The smart contract or authentication server then verifies the signature using the stored $H(K_d)$ or a public key (if asymmetric cryptography is used).

The full authentication request sent to the system is:

$$R = \{ID_d, T, N, \text{Sign}(K_d, ID_d \parallel T \parallel N)\}$$

3.3.3. Step 3: AI-Driven Risk Assessment

- Upon the attempt of a registered device to join the network, it issues an authentication request R. This request identifies the device identifier ID_d, a timestamp T, a nonce N (to prevent replay When the AI Authentication Server receives an authentication request, it evaluates the security risk of the request. A machine learning model processes various contextual factors, including previous user behavior, device type, network type, and geolocation. The computed *risk score RS* determines the authentication level to be executed: attacks), and a digital signature produced using K_d. The authentication request is then transmitted securely to the authentication server to be verified:

  $$RS = f(ID_d, T, N, \text{Behavioral Data})$$

  where f is a Random Forest trained on authentication logs. If the computed *risk scor*e is *below* the predefined threshold $T_{\text{threshold}}$, the request proceeds to blockchain validation. Otherwise, additional authentication steps are required. In our implementation, the function f computes the risk score RS for an authentication attempt. This function is realized using a Random Forest that is trained on historical authentication data. The inputs to f include the device identifier (ID_d), timestamp (T), nonce (N), and a set of behavioral features ($\mathbf{X}$), such as the number of login attempts and time since the last login. The risk score RS is normalized to fall between 0 and 1, with higher values indicating greater risk. This approach allows the AI Authentication Server to quickly assess risk and adjust authentication measures in real time.

3.3.4. Step 4: Smart Contract Execution

- The authentication request is cross-checked with blockchain data to confirm that the requesting device is registered and that its credentials have not been breached. The smart contract confirms the identity of the device by verifying if ID_d and the saved hash of K_d equals the recorded values stored on the blockchain:

  $$\text{Verify}\,(ID_d, H(K_d)) \Rightarrow \text{Blockchain Lookup}$$

- If the verification is successful, the authentication request proceeds to the next step. Otherwise, the authentication attempt is rejected.

3.3.5. Step 5: Adaptive Multi-Factor Authentication (MFA)

Based on the *risk score evaluation*, the system dynamically adjusts the authentication requirements:

- If $RS < T_{\text{threshold}}$, the request is considered low-risk, and authentication proceeds without additional verification.
- If $RS \geq T_{\text{threshold}}$, the system enforces an additional authentication factor, such as biometric authentication or a one-time password (OTP):

$$\text{Require(Biometric, OTP)}$$

- If the user successfully completes MFA verification, authentication is granted. Otherwise, access is denied.

3.3.6. Step 6: Secure Session Establishment

Once authentication is approved, the device establishes a secure session using encryption protocols to protect subsequent communications. The authentication event, along with the session details, is recorded immutably on the blockchain:

$$\text{Encrypt}\,(\text{Session Data}) \Rightarrow \text{Secure Session}$$

$$\text{Record}\,(ID_d, T, N, \text{Session Established}) \Rightarrow \text{Blockchain Entry}$$

3.3.7. Step 7: Continuous Monitoring and Anomaly Detection

During the authenticated session, the AI Authentication Server continuously monitors user behavior to detect anomalies. If any suspicious activity is detected, the system dynamically adjusts authentication requirements or terminates the session. The anomaly detection function is defined as:

$$\text{Anomaly Detection} = g(\text{Behavioral Data})$$

where g is a machine learning-based anomaly detection model.

3.3.8. Step 8: Secure Session Termination

When the user completes their activities, the session is securely terminated, and an entry is recorded on the blockchain:

$$\begin{aligned}&\text{TerminateSession}(ID_d) \Rightarrow \\ &\qquad\qquad \text{Record}\,(ID_d, T, N, \text{Session Terminated}) \Rightarrow \text{Blockchain Entry}\end{aligned}$$

This ensures a secure log of all authentication events, maintaining an immutable audit trail.

In summary, the TL2AB framework integrates advanced technologies to create a robust, lightweight authentication solution that addresses the unique challenges posed by 6G networks. The following sections will provide more details on the mathematical models that are used in the framework and discuss their security and performance evaluations.

4. Experimental Evaluation

4.1. Dataset

The synthesized dataset that we have created is rich in key features representing, at each authentication request, important information with regard to device details, user behavior metrics, and network characteristics. These features are crucial to construct a predictive model aimed at evaluating the risk associated with each authentication attempt. Tab. 4 describes each feature in the dataset, including its importance and relevance to the analysis conducted in this study. This complete dataset forms the basis of our machine learning model, from which meaningful insight into authentication patterns and possible security threats can be drawn.

4.1.1. Analysis of Authentication Dataset

Here, we provide a series of visualizations that develops the authentication data against various dimensions, including, risk score distribution, network types, device types, authentication methods, and relationships between login attempts, time since last login, and the calculated risk score.

- *Distribution of Risk Scores*: Fig. 3 illustrates the risk score distribution of authentication attempts. The histogram reveals a right-skewed distribution, indicating that there are many low-risk scores in most authentication instances, and high-risk cases are relatively infrequent. This distribution informs us that there would be majority of authentication attempts that would fall into low-risk classes, with a small percentage that would have to be examined in depth. The superimposed density curve over the histogram provides a smoothed estimate of the probability distribution, in support of the observation that risk scores are very dense in the lower range. This finding validates the objective of the research by revealing how the process of authentication

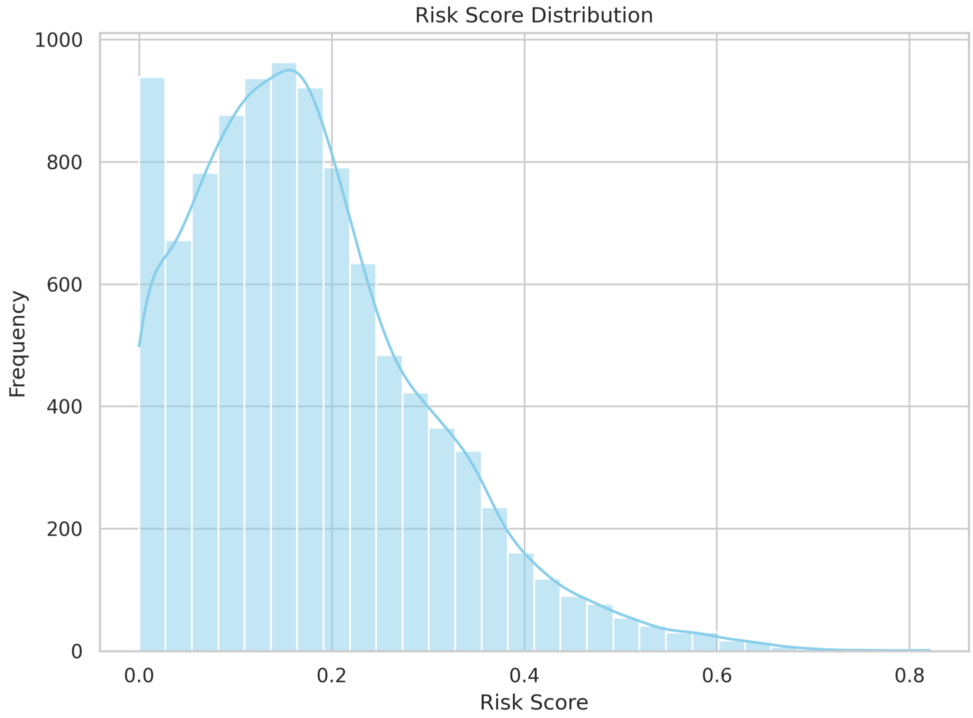


Figure 3: Risk Score Distribution

effectively identifies and identifies low-risk and high-risk authentication processes. The largely minor rate of high-risk incidents indicates that the proposed technique saves unnecessary security steps without dropping its guard about potential fraudulent access attempts. The risk score, calculated based on factors such as login attempts, time since last login, unusual activity, roaming, and VPN usage, has the distribution reported in Tab. 5

These statistics show that the risk scores are generally low, with a mean value of 0.1769 and most values concentrated below 0.25. The maximum value of 0.8794 indicates some high-risk users, although they are a minority. A small fraction of the total dataset (5.03%) is flagged for unusual activity. And Only 0.10% of the users are classified as high-risk, with risk scores above 0.7. This indicates that while most users have low risk scores, there is a very small group that exhibits behavior potentially indicative of higher security concerns.

- *Network Type Distribution:* Figure 4 shows the distribution of network types used in authentication attempts. The 4G, 5G, and WiFi networks are the three types considered. As seen from the results, authentication attempts are evenly distributed among network types so that the testing of the authentication framework accounts for different network conditions. This diversity is required for studying the impact of network variability on authentication performance, particularly for 6G networks. By adding network diversity to the evaluation, the study ensures that the proposed model is robust to network-level variations. This is consistent with the research objective of developing a flexible authentication system that works efficiently under heterogeneous network conditions, a key characteristic of 6G security.

- *Device Type Distribution:* Fig. 5 shows the distribution of device types in the dataset, which illustrates the relative frequency of authentication attempts from various device categories, such as laptops, smartphones, IoT sensors, and tablets. The findings show a relatively balanced distribution across device types, which implies that the dataset includes varied device characteristics. This distribution is important for evaluating the flexibility of the proposed authentication framework across different device ecosystems in a 6G network environment. These results validate the framework's ability to generalize as it is tested and

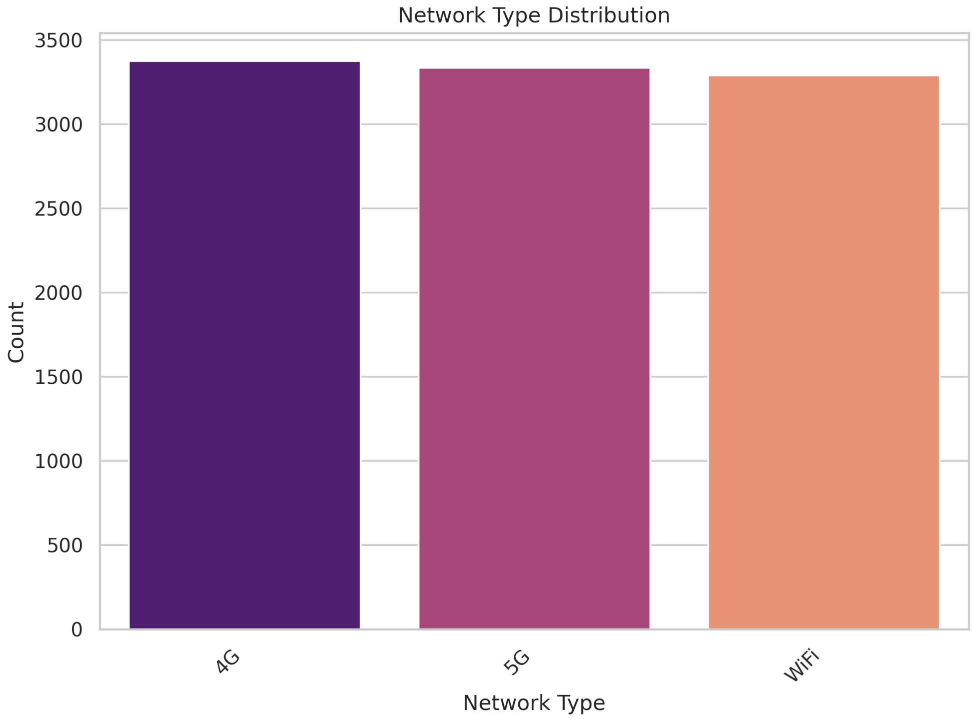


Figure 4: Network Type Distribution

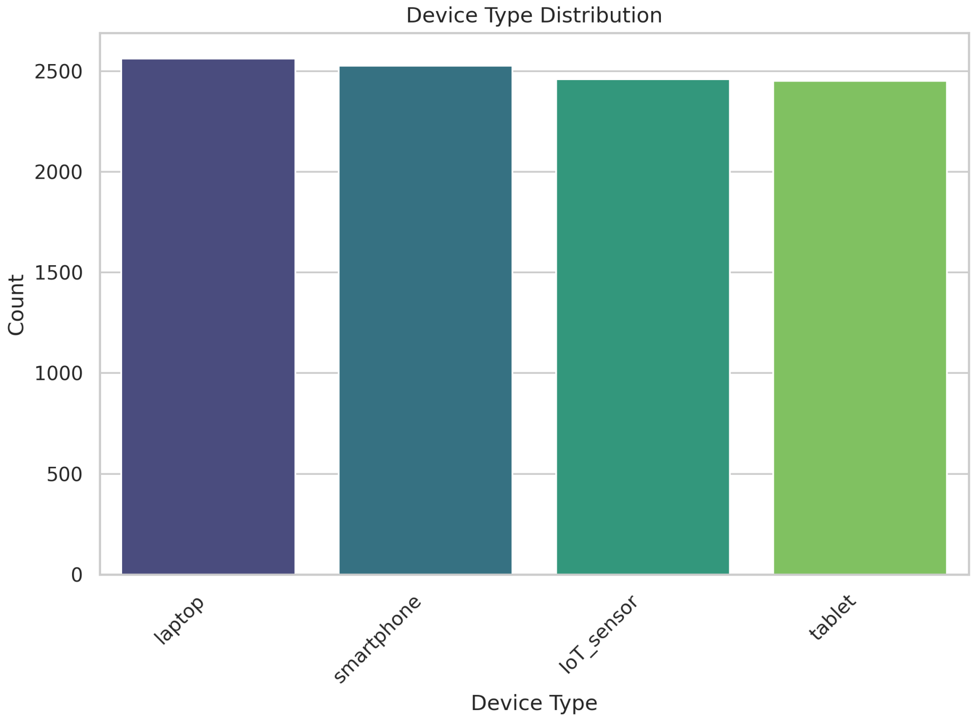


Figure 5: Device Type Distribution

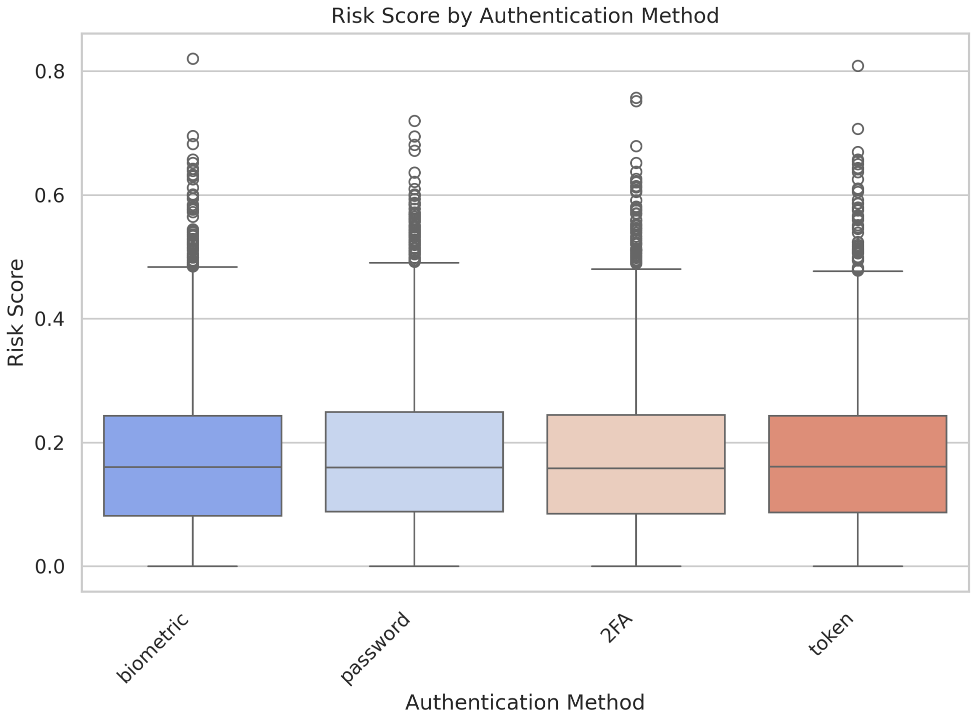


Figure 6: Risk Score by Authentication Method

trained across a broad range of devices. The balanced device type representation eliminates any single category from overwhelming the authentication model, and hence making it more suitable for real-world usage.

- *Risk Score by Authentication Method* Fig. 6 illustrates comparative risk score analysis for different authentication mechanisms, including biometric authentication, passwords, two-factor authentication (2FA), and token-based authentication. The box plot illustrates the risk score distribution for each authentication mechanism, with an indication of outliers and risk level variation. Findings reveal that some authentication mechanisms possess lower median risk scores, whereas other authentication mechanisms possess greater risk variability. This contrast highlights the necessity for the selection of robust authentication methods in order to secure 6G networks.

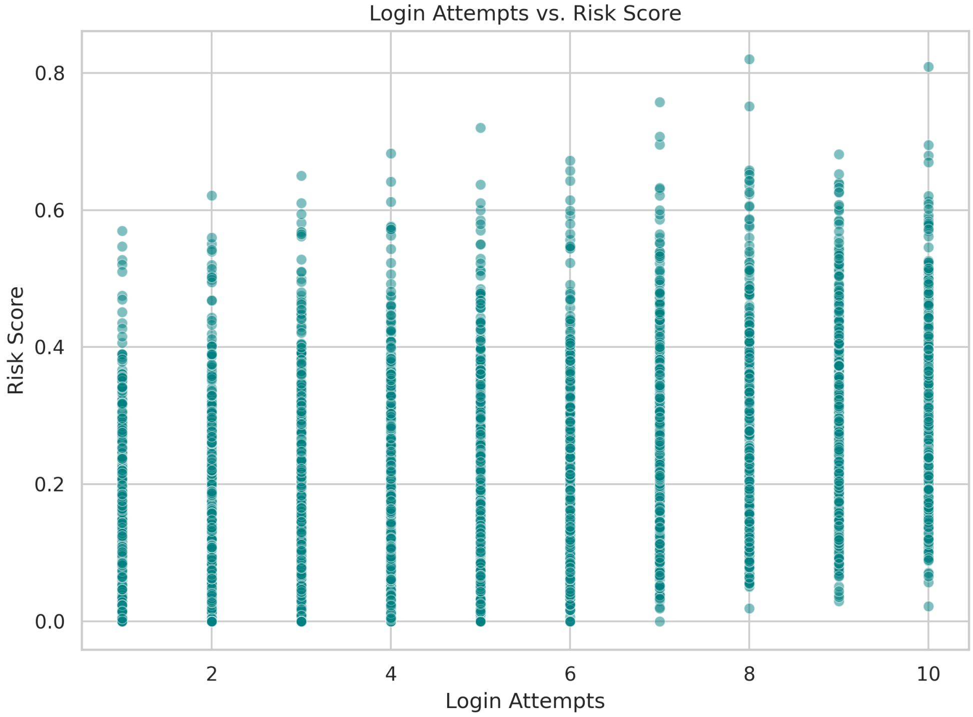


Figure 7: Login Attempts vs. Risk Score

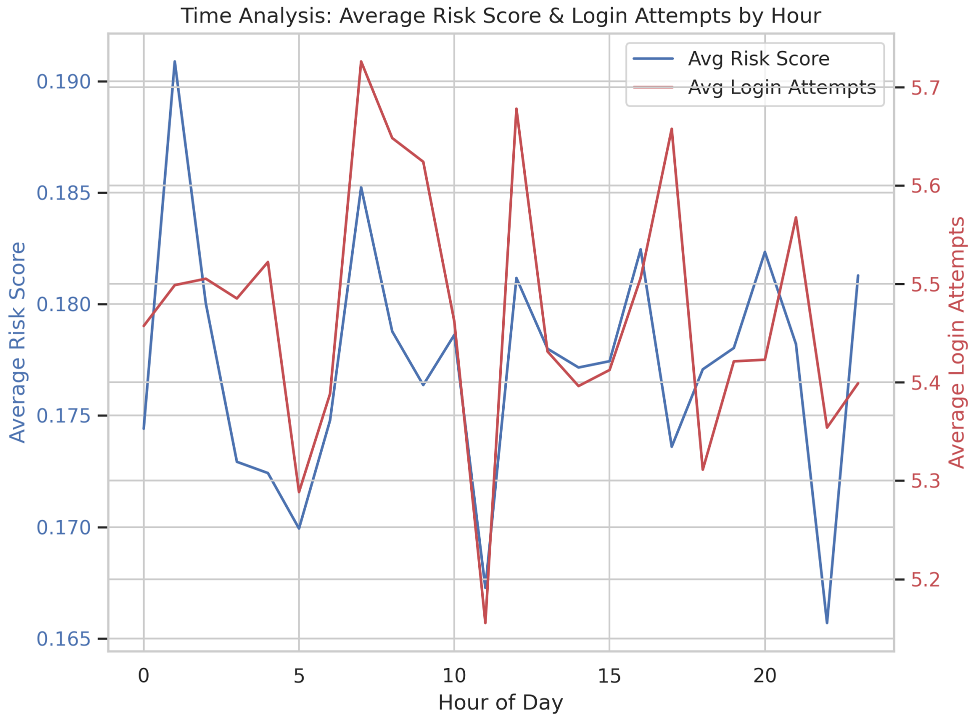


Figure 8: Login Attempts vs. Risk Score

- *Login Attempts vs. Risk Score* Fig. 7 displays the day-by-day variation in the risk scores and login attempts. The two-axis plot traces the trajectory of the average risk score (left y-axis) and the frequency of login attempts (right y-axis) throughout the day over 24 hours. The trends reflect periodic surges in login attempts, often after changes in risk scores. These findings highlight the necessity of considering time in authentication risk assessment. The trends suggest that authentication requests at particular time intervals may be inherently riskier, thus, dynamic security policies could be a requirement. This observation clearly supports the objective of the research to create a risk-aware authentication system. The possibility of identifying and bringing to attention suspicious activity based on failed login attempts enhances the system's performance in barring unauthorized access with minimal inconvenience to legitimate users.

- *Temporal Analysis of Risk Scores and Login Attempts* Fig. 8 graphs the temporal variation in risk scores and login attempts throughout the day. The two-axis graph displays fluctuations in the mean risk score (left y-axis) and the rate of login attempts (right y-axis) on a 24-hour cycle. The periodic login attempt peaks are discovered to regularly coincide with risk score oscillations. This temporal analysis casts critical light on authentication behaviors, and time-aware security controls can be designed to react to the change in user activity patterns based on this temporal analysis.such as the user profile or location of the attempt. These results emphasize the significance of including temporal considerations in authentication risk assessment. The trends in the observations imply that authentication requests within specific time windows could be riskier in nature, which would require dynamic security policies. This reinforces the study's aim by indicating the necessity of time-aware risk countermeasures in 6G authentication systems.

  Some login attempt levels (like 3, 5, and 8) show a few instances of higher risk scores (above 0.6), which might point to unusual behavior patterns around these attempt counts. The average number of login attempts by device type is as follows:

  The average number of login attempts for each device type is close to 5.5, as presented in Tab. 6, indicating that users across different devices and locations tend to make a similar number of attempts.

4.2. AI Authentication Server Evaluation

This part describes the AI model that, within the scope of TL2AB, assesses the risk associated with authentication attempts. The model is based on an ensemble learning technique known as *Random Forest* [18], which combines the predictions of multiple decision trees to improve the accuracy and robustness of the predictions. Unlike traditional models such as linear regression, Random Forest does not rely on a single hypothesis but rather aggregates multiple decision trees to make predictions. Our model uses a *Random Forest* in order to predict a risk score based on several features extracted from the data of authentication requests. According to this, the AI model loads the data, pre-processes it, trains the model, and does performance evaluations.

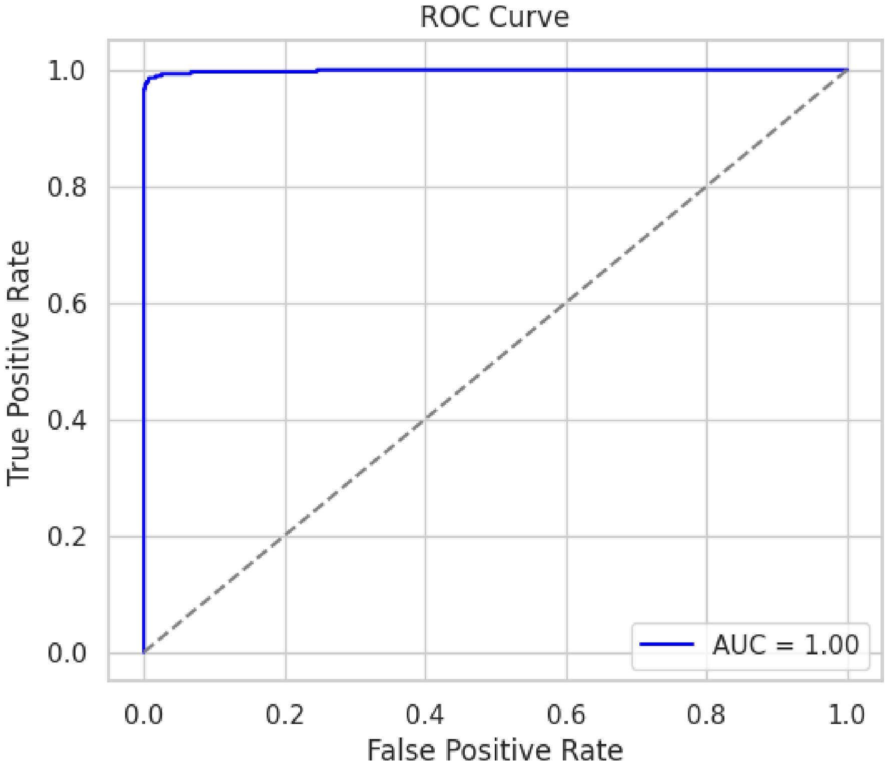


Figure 9: RoC Curve

4.2.1. Data Preprocessing and Feature Engineering

Before training the Random Forest model, several preprocessing steps are performed on the data to ensure that the model receives high-quality input. The preprocessing pipeline includes timestamp conversion, feature extraction, and one-hot encoding of categorical variables. The data preprocessing pipeline consists of several steps aimed at preparing the authentication data for model training. Categorical features such as ‘Network_Type‘, ‘Device_Type‘, ‘OS_Version‘, and ‘Authentication_Method‘ are transformed using one-hot encoding to convert them into a numerical format appropriate for machine learning algorithms. To mitigate the risk of overfitting and preserve model generalizability, features such as ‘Timestamp‘, ‘Device_ID‘, ‘IP_Address‘, ‘Location‘, and ‘App_Version‘ are excluded from the dataset. The remaining attributes are retained for model training.

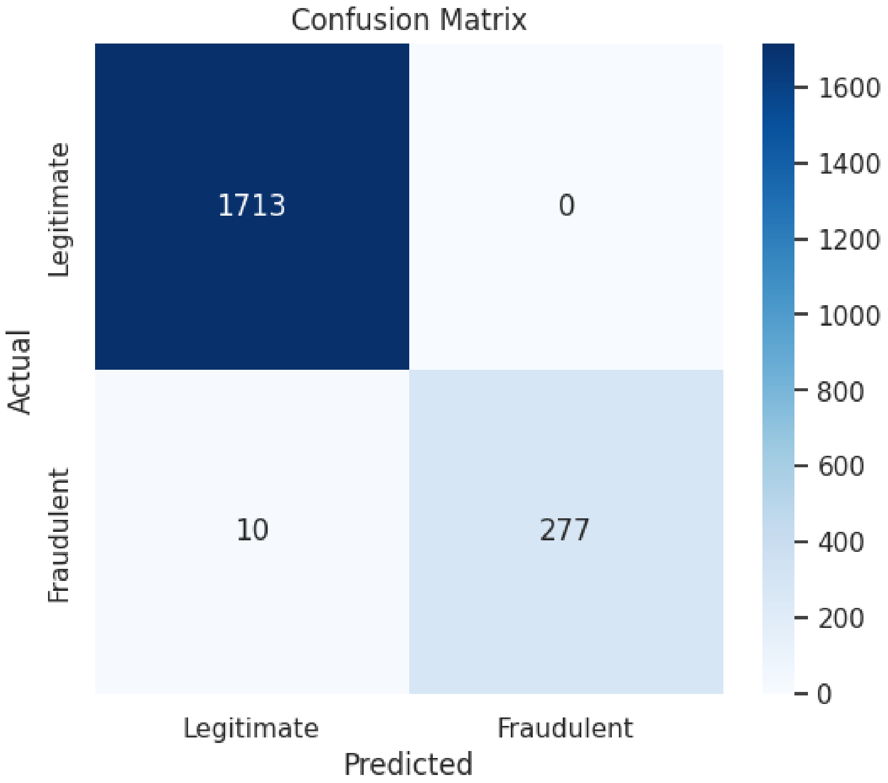


Figure 10: Confusion Matrix

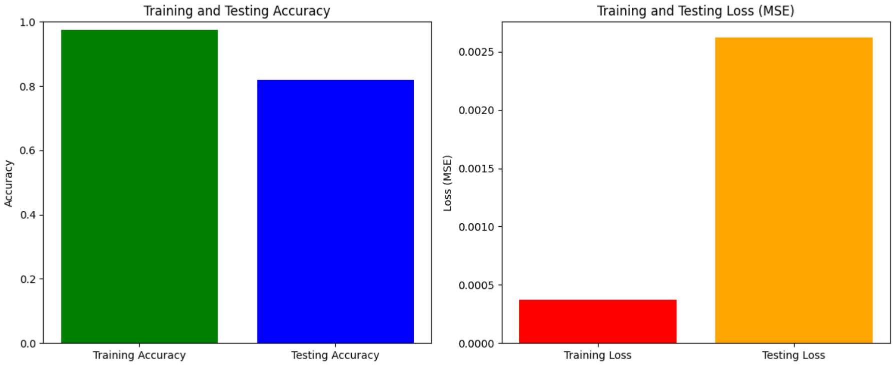


Figure 11: Training and Testing Accuracy and Loss

The model trained was a Random Forest (Tab. 7), accuracy and loss metrics were used to measure its performance in both the training and testing phases, as shown in Fig. 11, Fig. 9, and Fig. 10. The high training accuracy of the fraud detection model is 97.51%, , as shown in Fig. 11, indicating it acquires patterns from the training data very effectively. This trend is also accompanied by a training loss of 0.0004 and a test loss of 0.0026. Although the training loss is amazingly low, greater test loss assures that the model is not generalizing completely but has scope for improvement.

With regard to accuracy in detecting fraud, precision 99% reflects no false positive and no true transactions being flagged as fraud. The recall 0.965, however, reflects 3.5% true fraud cases that are not detected. The 0.997 AUC-ROC value guarantees that the model can effectively distinguish between fraudulent and legitimate cases.

False Negative Rate (FNR) of 0.035, i.e., only 3.5% of fraudulent transactions are missed. The False Positive Rate (FPR) is 0.000, which is good as it avoids unnecessary disruptions for legitimate users.

These metrics indicate that the lightweight Random Forest inside the AI authentication server can give accurate predictions and good performance on the training dataset and very commendable accuracy on the test dataset. The results are therefore suggestive of the model's effectiveness in capturing the underlying relationships in the data while making sure of a decent level of generalization.

5. Security Analysis

In this section, we provide a security analysis of the TL2AB authentication framework against all major attack vectors applicable in 6G networks.

6. Threat Model

In designing TL2AB, we assume a hostile environment characteristic of large-scale 6G networks. Our threat model considers both external and internal adversaries and quantifies the risks by examining the multi-layered defenses incorporated into our scheme. In particular, we address several potential attack vectors as follows:

Insider Attacks: A legitimate insider, such as a network administrator or user of a compromised device, may employ valid access to abuse privileges or steal confidential data. To mitigate this threat, cryptographic keys (K_d) are generated within and securely stored in a Trusted Execution Environment (TEE) or hardware security module (HSM), thereby minimizing exposure of sensitive credentials. Apart from that, real-time AI-driven anomaly detection monitors access patterns and sends alerts on the identification of suspicious activity, and role-based and attribute-based access controls ensure that insiders possess only the minimum privilege necessary for their roles.

Sybil Attacks: An attacker can create numerous pseudo-identities in an attempt to breach the distributed blockchain consensus or spam the system with fake authentication requests. Our protocol prevents this attack by having a rigorous procedure of identity verification at the device registration point, which ties every device's cryptographic key (K_d) to its physical identifier. Furthermore, the enormous computational and operational cost involved with registering large numbers of false identities, combined with a verification procedure demanding supermajority consensus (typically $> \frac{2}{3}$ of the nodes), significantly reduces any impact from fake identities.

Collusion and Multi-Node Compromise: The risk of multiple compromised nodes or colluding attackers attempting to compromise the blockchain or the AI Authentication Server is mitigated by the decentralized nature of TL2AB, which spreads the authentication load across geographically and logically distributed nodes. In addition, the robust consensus mechanism prevents any block from being authenticated unless a majority (e.g., 67% honesty) of nodes agree, thereby significantly reducing the likelihood of successful collusion attacks.

Replay Attacks: In a replay attack, an adversary intercepts a valid authentication request and replays it to gain unauthorized access. TL2AB defends against this threat by incorporating timestamps (T) and nonces (N) into each authentication request. These elements are verified against a narrow acceptance window and a record of previously used values, ensuring that stale or duplicated requests are promptly rejected. Dynamic session management further invalidates replay attempts by continuously adjusting authentication requirements in real time.

6.1. Security Requirements:

In pursuit of providing robust security against the threats above, TL2AB is architected to satisfy rigorous security properties. *Confidentiality* is maintained through effective use of strong encryption and secure storage methods that prevent leakage of sensitive data and keys. *Integrity* is provided by digitally signing every authentication event and storing it on an unalterable blockchain ledger so that any effort at tampering would be evident in real-time. Multifactor authentication and behavior verification with the use of artificial intelligence verify that only registered devices have access and provide non-repudiation, and a decentralized architecture and distributed consensus mechanism provide high *availability* as well as Denial-of-Service (DoS) or multi-node resistance. *Forward secrecy* is provided through independent and dynamic session key generation, such that the compromise of any single key does not pose a risk to previous sessions. Overall, persistent monitoring and responsive countermeasures provide TL2AB with the robustness to detect and mitigate new threats efficiently.

6.2. Security Analysis

6.2.1. Man-in-the-Middle (MITM) Attacks

Claim 1: We claim that the probability of success of an Man-in-the-Middle (MITM) attack is negligible.

Proof: To prove that a successful MITM attack has a negligible probability, we look in detail at the steps that an attacker, A, would have to go through. For this, it would intercept the message R, $ID_d, T, N, \text{sign}(K_d)$, where ID_d is the identity, T is the timestamp, N is a nonce, and $sign(K_d)$ is the cryptographic signature. Having intercepted R, he would then need to modify this message in such a way as to do it without modification being detected through the security mechanisms involved. After that, the attacker would have to breach the AI-based risk assessment layer, which is a constant monitoring of the system for anomalies. Finally, this would involve compromising the blockchain to change the stored authentication record associated with R. The overall probability of a successful MITM attack, denoted as $P(\text{MITM})$, can therefore be expressed as the product of the probabilities of successfully completing each of these steps: $P(\text{MITM}) = P(\text{Intercept}) \cdot P(\text{Modify}) \cdot P(\text{Bypass AI}) \cdot P(\text{Compromise Blockchain})$.

Given the cryptographic protection afforded by the signing of R, the on-going AI monitoring of the system, along with the immutability of the blockchain, the probabilities of successfully completing each of these steps are extremely small. Hence, we consider the overall probability of a successful MITM attack, $P(\text{MITM})$, to be negligible.

6.2.2. Replay Attacks

TL2AB includes both timestamps (T) and nonces (N) in every authentication request for resisting replay attacks.

Claim 2: TL2AB is secure against replay attacks.

Proof: An adversary intercepts a valid authentication request $R = \{ID_d, T, N, \text{sign}(K_d)\}$ at time t;. For such a replay attack to be effective at any later time $t + \Delta t$, two conditions have to be met by the adversary.

First, the timestamp T must still be accepted as current at time $t + \Delta t$. This is already ameliorated in TL2AB, since the system uses a small acceptance window over timestamps. If the time difference Δt is larger than this acceptance window, the system will reject the request for being outdated, which prevents the replay. Second, the nonce N shall not have been used in any previous authentication request. TL2AB enforces that every nonce is unique; so even if an adversary replays the captured message, the system will find the duplication of the nonce value and discard the replay request.

As the window for accepting timestamps is decreasing while the uniqueness of nonces is still strictly enforced, the success probability of a replay attack decreases. Therefore, this implies security against that kind of attack.

6.2.3. Impersonation Attacks

TL2AB detects impersonation attacks through the device-specific cryptographic keys, K_d, and the AI-driven behavior analysis approach.

Claim 3: In TL2AB, the success rate for an impersonation attack is close to zero.

Proof: To conduct a successful impersonation attack, the adversary has to successfully pass several conditions: First, it must acquire or forge a valid cryptographic key K_d that uniquely maps to the respective device. This would specifically entail an adversary creating an authentication request R. In addition, the adversary has to be able to impersonate the legitimate user's behavioral patterns as analyzed by the AI-driven system, such that the AI-based behavioral checks are bypassed.

The overall probability of a successful impersonation attack, denoted as $P(\text{Impersonation})$, may be written as: $P(\text{Impersonation}) = P(\text{Obtain}K_d) \cdot P(\text{Pass Crypto}) \cdot P(\text{Mimic Behavior})$.

Because the solution assumes the use of secure key generation and storage within a TEE, an adversary's chance of obtaining or forging the cryptographic key K_d is minimized; therefore, $P(\text{Obtain } K_d)$ is considered negligible. This is further enforced by the fact that continuous AI-driven behavioral analysis monitors the unique behavioral pattern of the legitimate user to an extent that makes the likelihood of successfully mimicking the behavior, $P(\text{Mimic Behavior})$, very low. In light of such formidable security measures, we conclude that the overall probability of success in an impersonation attack $P(\text{Impersonation})$ is negligible.

6.3. Formal Security Analysis using BAN Logic

To further assure the security guarantees of TL2AB, we provide a formal analysis of the authentication protocol using BAN logic. The logic allows us to reason about the beliefs that are established between communicating principals after the execution of a cryptographic protocol. In our scenario, we have two principals: the user device D and the authentication server or smart contract S. The message of interest is the authentication request:

$$D \to S : \{ID_d, T, N, \text{Sign}_{K_d}(ID_d \parallel T \parallel N)\}$$

We define the following BAN logic primitives:

- P **believes** X: Principal P believes statement X
- P **sees** X: Principal P receives message X
- P **once-said** X: Principal P said message X at some point in the past
- **fresh**(X): Message X is fresh
- **pubkey**(K, P): K is the public key of principal P

The following assumptions are made: (1) the server S believes it knows the authentic public key of the device D, i.e., S **believes pubkey**(K_d, D); (2) the server believes that the nonce N is fresh, i.e., S **believes fresh**(N); and (3) the server receives the signed message, i.e., S **sees** $\mathrm{Sign}_{K_d}(ID_d \parallel T \parallel N)$.

Based on these assumptions and the rules of BAN logic, the server concludes the following: from the digital signature and its belief in the key binding, S **believes** D **once-said** $(ID_d \parallel T \parallel N)$. Given the freshness of the nonce, it follows that S **believes** D **believes** $(ID_d \parallel T \parallel N)$, and therefore, S **believes** $\mathrm{auth}(D)$; that is, the server is convinced that the request originated recently and authentically from device D. This formal reasoning confirms that the authentication phase of TL2AB ensures origin authenticity and freshness, and is resilient to replay attacks.

6.3.1. Denial of Service (DoS) Attacks

The decentralized nature of blockchain and the adaptive risk assessment by AI provide inherent resistance to Denial of Service (DoS) attacks.

Claim 4: TL2AB significantly mitigates the impact of DoS attacks compared to centralized authentication systems.

Proof: In a traditional centralized authentication system, a successful DoS attack typically involves overwhelming the central server with an excessive amount of traffic, causing the system to become unavailable. The probability of a successful DoS attack in a centralized system can be expressed as:

$$P(\mathrm{DoS}_{\mathrm{centralized}}) = P(\mathrm{Overwhelm\_central\_server}),$$

where $P(\mathrm{Overwhelm\_central\_server})$ is the likelihood of overloading the single point of failure in a centralized system — the central server.

In contrast, TL2AB employs a decentralized architecture based on blockchain, which distributes authentication tasks across multiple nodes. For a DoS attack to succeed against TL2AB, the adversary would first need to overwhelm multiple blockchain nodes simultaneously. Additionally, the adversary must bypass the AI's adaptive risk assessment system, which detects unusual traffic patterns and adjusts defenses dynamically. Thus, the probability of a successful DoS attack in TL2AB is given by:

$$P(\mathrm{DoS}_{\mathrm{TL2AB}}) = P(\mathrm{Hit\_multiple\_nodes}) \cdot P(\mathrm{Bypass\_AI}),$$

where $P(\text{Hit\_multiple\_nodes})$ represents the difficulty of attacking multiple blockchain nodes concurrently, and $P(\text{Bypass\_AI})$ accounts for the challenge of evading the AI's adaptive monitoring.

Due to the distributed nature of the blockchain network and the AI's ability to detect and respond to abnormal traffic patterns, the probability of a successful DoS attack in TL2AB is significantly lower than that in a centralized system. Therefore, we can conclude that $P(\text{DoS}_{\text{TL2AB}}) \ll P(\text{DoS}_{\text{centralized}})$, which demonstrates TL2AB's superior resistance to DoS attacks.

6.4. Privacy Preservation

TL2AB ensures user privacy through several mechanisms. First, cryptographic keys are managed within a Trusted Execution Environment (TEE), which prevents unauthorized access and protects sensitive data. Second, the AI component analyzes behavioral patterns without storing raw user data, thereby minimizing privacy risks associated with data collection. Lastly, the inherent pseudonymous nature of blockchain transactions provides an additional layer of privacy, making it difficult to trace activities back to individual users. The TL2AB framework incorporates multiple layers of privacy-preserving mechanisms to protect sensitive information:

- **Key Privacy:** Cryptographic key K_d is never transmitted. A cryptographic hash $H(K_d)$ is stored on-chain, so it is computationally infeasible to derive the original key due to the one-way nature of hash functions. The key itself is stored securely within the Trusted Execution Environment (TEE).

- **Privacy of Behavioral Data:** Locally or by a privacy-oblivious AI model, the risk is assessed. Only the derived features, such as login frequency or location region (and not raw behavioral logs), are employed so that raw user activity and personal data do not leak.

- **On-Chain Privacy:** Information that is stored on-chain is limited and minimal in scope and includes hashed or insensitive values only. No personally identifiable information (PII) is ever stored on-chain.

These measures collectively ensure that TL2AB protects user privacy across three fronts: device identity, behavioral context, and cryptographic material, even in an adversarial environment with partial visibility into the network or blockchain.

Claim 5: TL2AB preserves user privacy with high probability.

Proof: Let E represent the event of a privacy breach. The probability of event E occurring can be expressed as: $P(E) = P(\text{TEE\_compromised}) \cdot P(\text{AI\_data\_leaked}) \cdot P(\text{Blockchain\_deanonymized})$. Given the strong security properties of the TEE, the data minimization approach utilized in the AI analysis, and the pseudonymous nature of blockchain transactions, each of these probabilities is very low. Therefore, the overall probability of a privacy breach, $P(E)$, is negligible.

6.5. Forward Secrecy

TL2AB ensures forward secrecy through dynamic session key generation and continuous risk assessment.

Claim 6: TL2AB provides forward secrecy. **Proof:** Let S_i and S_j denote two distinct sessions, where $i < j$. The compromise of the session key K_j does not reveal any information about the session key K_i. This is due to several factors: First, session keys are generated independently for each session, ensuring that the compromise of one does not affect the others. Second, the AI component continuously updates the risk assessment, which influences the key generation process, further enhancing security. Lastly, the blockchain records each authentication event separately, making it more challenging for an adversary to link compromised keys across sessions.

As a result, we can express the relationship between the probabilities as: $P(\text{Compromise\_}S_i|\text{Compromise\_}S_j) \approx P(\text{Compromise\_}S_i)$, demonstrating that the compromise of one session key does not compromise the security of others, thereby ensuring forward secrecy.

In conclusion, this formal security analysis demonstrates that TL2AB provides security guarantees against a wide range of attack vectors relevant to 6G networks. The integration of AI and blockchain technologies creates a synergistic effect, significantly enhancing the overall security posture of the authentication framework.

6.6. Comprehensive Analysis of TL2AB Capabilities

In this part, we provide an in-depth evaluation of the benefits of TL2AB by taking into account its security, privacy guarantee, dynamism in dynamic environments, and international scalability and responsiveness. We then compare these elements to the similar state-of-the-art authentication paradigms.

6.6.1. Scalability and Performance

TL2AB is a lightweight architecture designed specifically for computation-limited IoT devices in 6G networks. With the deployment of decentralized blockchain technology, TL2AB divides authentication operations among various nodes, hence eliminating single points of failure as well as guaranteeing high availability. Moreover, the integration of AI-driven ongoing risk analysis lessens computational overhead while maintaining low latency despite dynamic network conditions.

6.6.2. Security Features

TL2AB achieves robust security by integrating multiple layers of defense. The use of blockchain ensures tamper-proof logging and distributed trust, while cryptographic signatures and secure key storage (within a Trusted Execution Environment using salted hashes) protect sensitive credentials. Additionally, the AI Authentication Server continuously monitors device behavior to assess risk and detect potential anomalies dynamically. This multifaceted approach provides strong resilience against attacks such as man-in-the-middle, replay, impersonation, and denial-of-service.

6.6.3. Privacy-Preserving Mechanisms

To ensure the privacy of users, TL2AB employs various privacy-enhancing practices. Privacy-sensitive information is protected by keeping salted hashes of cryptographic keys rather than plaintext keys, and each blockchain transaction is pseudonymous to prevent direct linking with individual users. Moreover, the AI component processes the behavioral data in a minimized data fashion without keeping plaintext personal data, thereby minimizing privacy exposure.

6.6.4. Adaptability and Dynamic Response

One of the key strengths of TL2AB is that it is highly flexible. The artificial intelligence-based risk assessment in the framework adapts continuously in real time, allowing the system to dynamically change authentication requirements based on current threat levels. This makes the system responsive to changing network conditions and evolving threats, while maintaining a balance between security and usability without overloading the computation.

6.6.5. Comparative Analysis with Related Frameworks

Table 9 provides a qualitative comparison of TL2AB with several related authentication schemes from the literature. The comparison is based on four key criteria: security robustness, privacy preservation, adaptability, and scalability/performance.

This comprehensive analysis demonstrates that TL2AB not only surpasses the security, privacy, and flexibility but also makes significant improvements in scalability and performance over existing state-of-the-art frameworks. The integration of blockchain technology with AI-based continuous monitoring makes TL2AB a robust and flexible instrument for 6G networks.

7. Advantages of TL2AB

While the works reviewed above in the related works section contribute to knowledge in one way or another, TL2AB differs in that it incorporates AI-driven continuous monitoring with blockchain for developing a decentralized authentication framework. The solution designs so far have been for specific applications or technologies, while TL2AB is intended to be applied holistically in various 6G environments. Including the following advantages:

- *Efficiency and Resource Utilization:* Unlike the three-factor mechanism proposed in the health sector [6], TL2AB is lightweight; hence, more suitable for resource-constrained IoT devices prevalent in the 6G networks.

- *Decentralization:* The fallback to a single, central system in the CL-UCSSO mechanism and other proposals presents some concern due to a single point of failure [6, 8]. TL2AB enhances a blockchain-based platform that will support a distributed model of trust.

- *Adaptability:* The lightweight protocols put forward in maritime transportation and satellite-ground networks rely mostly on specific contexts. TL2AB uses AI for continuous adaptation to emerging threats, with a more robust security posture.

The comprehensive security framework TL2AB, combines multi-factor authentication and blockchain into one platform that enables dynamic and context-aware authentication in diversified applications in 6G. The proposed TL2AB tends to fill those gaps identified in the literature review by providing a flexible and efficient, robust authentication solution that could be scaled up with growing demands of the 6G network without compromising security and privacy.

7.1. Scalability and Performance

Scalability and efficiency are crucial factors in 6G networks, especially when handling billions of devices. Works like Tao et al. [7] and Fang et al. [10] focus on optimizing protocols to handle large-scale networks by minimizing overhead, reducing latency, and ensuring rapid authentication. This focus aligns with TL2AB's goal of providing a lightweight, scalable authentication mechanism that can adapt to large, dynamic 6G environments. Tab. 8 summarizes the key aspects of the related works and their comparison to the TL2AB framework.

7.2. Computational and Communication Performance Comparison

In this part, we compare the computation and communication efficiency of TL2AB with other authentication methods. Tab. 10 illustrates a comparison of the reported computation and communication in various works.

Our model requires 1.7202 seconds for training and 0.000375 seconds per sample for inference, which indicates efficient processing. The inference CPU utilization is 21% measured, indicating a modest computation cost sufficient for real-time authentication in 6G networks. TL2AB also has a tiny model size of 0.15 MB, making it light-weight as opposed to deep-learning-based authentication systems.

The whole length of the message transmitted via the authentication in the TL2AB protocol is 334 bytes, which include the authentication request (296 bytes), risk assessment response (5 bytes), smart contract verification response (1 byte), and session confirmation (32 bytes). The message length is still small in a step to decrease communication overhead without compromising security and scalability within high-speed networks. As regards communication efficiency, TL2AB transmits 334 bytes while authenticating with virtually negligible overhead. While Aman et al. [16] has a smaller message length of 40 bytes, they are utilizing the classic cryptographic schemes that do not necessarily have more flexibility while handling dynamic 6G environments. On the contrary, Al Ahmed et al. [15] have extremely high encryption delay (0.077642 sec) and decryption time (3.537678 sec), which would induce authentication delay in real-time systems.

Compared to Siddhartha et al. [12], with a total computational energy consumption of 102.059 mJ, TL2AB's AI-based lightweight approach minimizes computation without increasing communication overhead. Similarly, Tahir et al. [17] obtained 5.2% reduction in computational overhead and 3.8% reduction in communication overhead, and TL2AB offers a compromise among security, efficiency, and real-time flexibility. That is, TL2AB is an efficient authentication scheme with low computational and communication overhead, efficient, secure, and fast authentication, and therefore appropriate for future 6G networks.

8. Conclusion

In summary, the TL2AB authentication framework offers a fresh paradigm for solving the challenging security issues caused by the emergence of 6G technology. TL2AB merges artificial intelligence with blockchain, proposing a lightweight, efficient, and robust authentication mechanism suitable for high-demand applications from several fields. Compared to the various authentication protocols that exist, TL2AB is way more efficient and secure. Future work will consider network scalability for TL2AB and explore any potential enhancements possible with emerging technologies like quantum cryptography. Ultimately, TL2AB should serve as a way in establishing secure and user-friendly authentication mechanisms in coming 6G networks to further enable advanced applications that require enhanced security and privacy.

Appendix A. Example Appendix Section

Appendix text.

References

[1] W. Jiang, B. Han, M. A. Habibi, H. D. Schotten, The road towards 6g: A comprehensive survey, IEEE Open Journal of the Communications Society 2 (2021) 334–366.

[2] S. Dang, O. Amin, B. Shihada, M.-S. Alouini, What should 6g be?, Nature Electronics 3 (1) (2020) 20–29.

[3] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, M. Ylianttila, The roadmap to 6g security and privacy, IEEE Open Journal of the Communications Society 2 (2021) 1094–1122.

[4] K. A. Alezabi, F. Hashim, S. J. Hashim, B. M. Ali, A. Jamalipour, Efficient authentication and re-authentication protocols for 4g/5g heterogeneous networks, EURASIP Journal on Wireless Communications and Networking 2020 (2020) 1–34.

[5] A. S. Khan, M. A. Sattar, K. Nisar, A. A. A. Ibrahim, N. B. Annuar, J. b. Abdullah, S. Karim Memon, A survey on 6g enabled light weight authentication protocol for uavs, security, open research issues and future directions, Applied Sciences 13 (1) (2022) 277.

[6] T.-V. Le, C.-F. Lu, C.-L. Hsu, T. K. Do, Y.-F. Chou, W.-C. Wei, A novel three-factor authentication protocol for multiple service providers in 6g-aided intelligent healthcare systems, IEEE Access 10 (2022) 28975–28990.

[7] Y. Tao, H. Du, J. Xu, L. Su, B. Cui, On-demand anonymous access and roaming authentication protocols for 6g satellite–ground integrated networks, Sensors 23 (11) (2023) 5075.

[8] S. A. Chaudhry, A. Irshad, M. A. Khan, S. A. Khan, S. Nosheen, A. A. AlZubi, Y. B. Zikria, A lightweight authentication scheme for 6g-iot enabled maritime transport system, IEEE Transactions on Intelligent Transportation Systems 24 (2) (2021) 2401–2410.

[9] J. Asim, A. S. Khan, R. M. Saqib, J. Abdullah, Z. Ahmad, S. Honey, S. Afzal, M. S. Alqahtani, M. Abbas, Blockchain-based multifactor authentication for future 6g cellular networks: A systematic review, Applied Sciences 12 (7) (2022) 3551.

[10] H. Fang, A. Qi, X. Wang, Fast authentication and progressive authorization in large-scale iot: How to leverage ai for security enhancement, IEEE network 34 (3) (2020) 24–29.

[11] D. Garabato, C. Dafonte, R. Santovena, A. Silvelo, F. J. Novoa, M. Manteiga, Ai-based user authentication reinforcement by continuous extraction of behavioral interaction features, Neural Computing and Applications 34 (14) (2022) 11691–11705.

[12] V. Siddhartha, G. S. Gaba, L. Kansal, A lightweight authentication protocol using implicit certificates for securing iot systems, Procedia computer science 167 (2020) 85–96.

[13] V. Kumar, N. Malik, J. Singla, N. Jhanjhi, F. Amsaad, A. Razaque, Light weight authentication scheme for smart home iot devices, Cryptography 6 (3) (2022) 37.

[14] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, L. Rafferty, A decentralized lightweight blockchain-based authentication mechanism for iot systems, Cluster Computing 23 (3) (2020) 2067–2087.

[15] M. T. Al Ahmed, F. Hashim, S. J. Hashim, A. Abdullah, Authentication-chains: blockchain-inspired lightweight authentication protocol for iot networks, Electronics 12 (4) (2023) 867.

[16] M. N. Aman, K. C. Chua, B. Sikdar, A light-weight mutual authentication protocol for iot systems, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.

[17] M. Tahir, M. Sardaraz, S. Muhammad, M. Saud Khan, A lightweight authentication and authorization framework for blockchain-enabled iot network in health-informatics, Sustainability 12 (17) (2020) 6960.

[18] S. J. Rigatti, Random forest, Journal of Insurance Medicine 47 (1) (2017) 31–39.

Feature	**Description**	**Type**
Timestamp	The timestamp when the authentication event occurred, randomly generated within a month.	DateTime
Device_ID	Unique identifier for each device.	String (ID)
IP_Address	Randomly generated IP address (e.g., 192.168.1.1).	String (IPv4)
Location	Geographical coordinates (latitude, longitude) of the device's location, randomly generated.	String (Latitude, Longitude)
Network_Type	Type of network being used (WiFi, 4G, or 5G).	Categorical (WiFi, 4G, 5G)
Device_Type	Type of device used for authentication (smartphone, IoT sensor, laptop, or tablet).	Categorical (smartphone, IoT, laptop, tablet)
OS_Version	The version of the operating system on the device (e.g., iOS_15, Android_12).	Categorical (OS Version)
App_Version	Version of the application used for authentication (e.g., 1.2, 2.5).	String (Version)
Authentication_Method	Authentication method used (password, biometric, token, 2FA).	Categorical (password, biometric, token, 2FA)
Login_Attempts	The number of login attempts made during this session (between 1 and 10).	Integer (1–10)
Time_Since_Last_Login	Time in hours since the last successful login, ranging from 0 to 168 hours (7 days).	Numeric (Continuous)
Unusual_Activity_Flag	Flag indicating whether unusual activity was detected during the session (1: Yes, 0: No).	Binary (0, 1)
Is_Roaming	Flag indicating whether the user is roaming (1: Yes, 0: No).	Binary (0, 1)
Is_VPN	Flag indicating whether the user is using a VPN (1: Yes, 0: No).	Binary (0, 1)
Risk_Score	A calculated risk score based on multiple factors such as login attempts, time since last login, etc.	Numeric (0–1)

Table 4: Feature Descriptions

Statistic	**Value**
Count	100,000
Mean	0.1769
Standard Deviation	0.1237
Minimum	0.0000
25th Percentile (Q1)	0.0863
50th Percentile (Median)	0.1590
75th Percentile (Q3)	0.2431
Maximum	0.8794

Table 5: Risk Score Statistics

Device Type	**Average Login Attempts**
IoT Sensor	5.50
Laptop	5.51
Smartphone	5.49
Tablet	5.45

Table 6: Login Attempts by Device Type

Parameter	**Value**
Number of Trees (n_estimators)	100
Number of Features Used	23
Details of the first tree in the forest	
Tree depth	30
Number of leaves	4974
Number of nodes	9947

Table 7: Model Architecture

Paper & Application Domain	**Security Mechanism**	**Authentication Approach**	**Technological Focus**	**Scalability & Performance**
Le et al. [6] (Healthcare)	Data Privacy, System Cost Optimization	3-Factor Authentication (Smart Card, Password, Biometric)	Healthcare Networks, Authentication Protocols	High cost, secure but computationally expensive
Chaudhry et al. [8] (Maritime)	GPS Spoofing, Unauthorized Data Access	Lightweight Authentication Protocol	GPS-based Systems, Maritime Security	Low overhead, lightweight, secure
Tao et al. [7] (Satellite Networks)	Privacy Preservation, Energy Efficiency	Bilinear Pairing-based Group Signature, Batch Authentication	Satellite-ground Integrated Networks	Energy-efficient, scalable, low-latency
Asim et al. [9] (Blockchain)	MFA, Cyber Attack Prevention	Multi-Factor Authentication (MFA)	Blockchain-based Security	Blockchain-enhanced security, scalable
Fang et al. [10] (IoT)	Security Management, Authentication Efficiency	AI-Enabled Lightweight Authentication	IoT Networks, AI-enhanced Security	Scalable, adaptive to dynamic environments
Garabato et al. [11] (General)	Continuous Authentication, Activity Monitoring	AI-based Continuous Authentication (SVM, MLP, Deep Learning)	AI-driven Authentication, Continuous User Verification	Scalable, adaptive, continuous verification
TL2AB Framework (6G Networks)	Device Security, Risk Assessment	Lightweight & Dynamic Authentication (Cryptographic Signatures, AI-based Risk Assessment)	6G Networks, AI-driven Security	Scalable, low-latency, real-time dynamic adjustments

Table 8: Comparison of Authentication Approaches in 6G Networks

Table 9: Comprehensive Comparison of Authentication Frameworks

Reference	Security Robustness	Privacy Preservation	Adaptability	Scalability & Performance
Siddhartha et al. [12]	High; robust multi-factor security	Moderate; traditional key management	Low; static authentication model	Low; high computational overhead
Kumar et al. [13]	Moderate-High; efficient for smart home IoT	Moderate; limited to specific domain	Low; limited dynamic adjustment	Moderate; optimized for smart home devices
Khalid et al. [14]	High; decentralized blockchain-based security	Moderate; standard blockchain privacy	Moderate; fixed protocol parameters	Moderate; blockchain overhead may limit scalability
Al Ahmed et al. [15]	High; innovative consensus algorithm enhances security	Moderate; privacy not extensively addressed	Moderate; cluster-based but less dynamic	Moderate; efficient clustering with integration challenges
Aman et al. [16]	High; PUF-based mechanism provides strong security	High; intrinsic hardware-level privacy	Low-Moderate; less emphasis on dynamic adaptation	Low; optimized for constrained devices only
Tahir et al. [17]	High; robust for health informatics	High; designed for sensitive data	Moderate; fixed policies	Moderate; balanced performance for specialized applications
TL2AB (Proposed)	**Very High; combines blockchain and AI for continuous, dynamic threat assessment**	**Very High; employs salted hashes and pseudonymous transactions**	**Very High; real-time AI-driven adaptation**	**High; lightweight design ensuring low latency and high scalability**

Table 10: Comparison of Computational and Communication Performance with Related Works

Scheme	**Reported Results (Computation)**	**Reported Results (Communication)**
Siddhartha et al. [12]	Total computational energy: 102.059 mJ	Transmission energy per bit: 0.72 µJ, Reception: 0.81 µJ
Aman et al. [16]	Hash operations: O(n), Modular exponentiation: O(n + M(l)k)	Message length: 40 bytes, Lower overhead than traditional methods
Tahir et al. [17]	Computational overhead reduced by 5.2%	Communication overhead reduced by 3.8%
Kumar et al. [13]	AES delay: 0.001975 ms, SHA-1 delay: 0.001135 ms	Reported security increase with minimal impact on communication
Al Ahmed et al. [15]	RSA Encryption: 0.077642 sec, Decryption: 3.537678 sec	Average network delay: 7 ms
Our Model (TL2AB)	Training Time: 1.7202 sec, Inference Time: 0.000375 sec, CPU Usage: 21%, Model Size: 0.15 MB	Message length: 334 bytes (minimal overhead)

Title Page Template

Title:

TL2AB : Trusted Lightweight Authentication using AI and Blockchain for 6G Networks

Author Information

Author names:

Sabrina Sakraoui[a], Makhlouf Derdour[b], Ahmed Ahmim[c], Reham Almukhlifi[d], Marwa Ahmim [a], Insaf Ullah[e]

Affiliations:

[a]Networks and Systems Laboratory, Department of Computer Science, Badji Mokhtar Annaba University, , Annaba, 23000, , Algeria

[b]Department of Computer Science, Oum El Bouaghi University, Oum El Bouaghi, 4000, , Algeria

[c]Department of Computer Science, Mohamed-Cherif Messaadia University, Souk Ahras, 41000, , Algeria

[d]Cybersecurity Department, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia

[e]Institute for Analytics and Data Science, University of Essex, Essex, CO4 3SQ, , United Kingdom

Corresponding author:

Insaf Ullah

Institute for Analytics and Data Science, University of Essex, Essex, CO4 3SQ, , United Kingdom

Insaf.ullah@essex.ac.uk

For more information, please refer to the relevant sections under submission guidelines for the journal in the Guide for Authors.

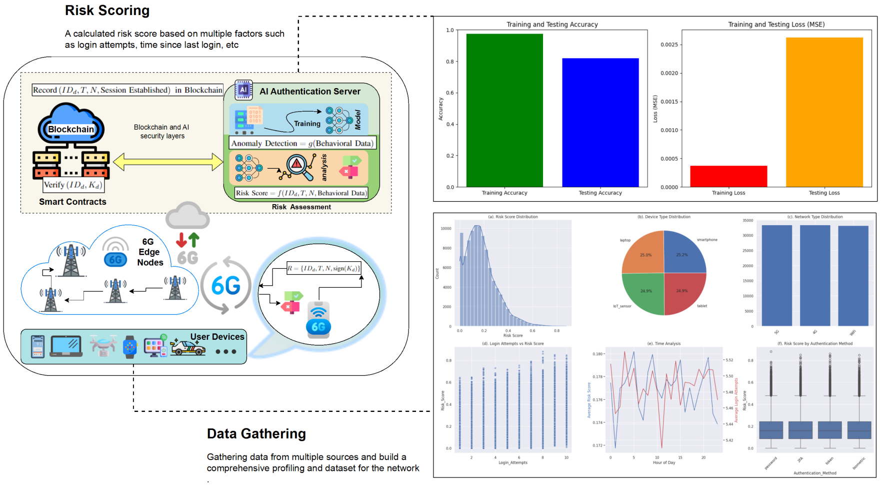
Highlights

TL2AB : Trusted Lightweight Authentication using AI and Blockchain for 6G Networks

- TL2AB introduces a new authentication scheme uniquely combining blockchain and AI technologies that is robust and lightweight for authentication mechanisms in 6G networks.
- The framework leverages blockchain's immutable and distributed architecture to enable decentralized authentication while using AI for real-time threat monitoring.
- Resource-efficient design specifically optimized for IoT devices makes TL2AB highly suitable for large-scale 6G deployments.
- AI-driven continuous authentication enables adaptive security responses without compromising the lightweight nature of the framework.

Graphical Abstract

TL2AB : Trusted Lightweight Authentication using AI and Blockchain for 6G Networks



Risk Scoring

A calculated risk score based on multiple factors such as login attempts, time since last login, etc

Data Gathering

Gathering data from multiple sources and build a comprehensive profiling and dataset for the network

Record $(ID_d, T, N, \text{Session Established})$ in Blockchain
Blockchain
Blockchain and AI security layers
Verify (ID_d, K_d)
Smart Contracts
AI Authentication Server
Training
Model
Anomaly Detection $= g(\text{Behavioral Data})$
analysis
Risk Score $= f(ID_d, T, N, \text{Behavioral Data})$
Risk Assessment
6G Edge Nodes
6G
$R = \{ID_d, T, N, \text{sign}(K_d)\}$
User Devices
Training and Testing Accuracy
Accuracy
Training Accuracy
Testing Accuracy
Training and Testing Loss (MSE)
Loss (MSE)
Training Loss
Testing Loss
(a). Risk Score Distribution
Count
Risk Score
(b). Device Type Distribution
laptop 25.0%
smartphone 25.2%
IoT_sensor 24.9%
tablet 24.9%
(c). Network Type Distribution
5G
4G
WiFi
(d). Login Attempts vs Risk Score
Risk_Score
Login_Attempts
(e). Time Analysis
Average Risk Score
Average Login Attempts
Hour of Day
(f). Risk Score by Authentication Method
Risk_Score
password
2FA
token
biometric
Authentication_Method