

VITA: Verifiable Decentralized Authentication and Access Control in B5G/6G IoT Environments

Mohammed B. Alshawki^{*†}, Yehao Zhou^{*}, Sándor Laki^{*}, Péter Ligeti^{*}

^{*}Faculty of Informatics, ELTE Eötvös Loránd University, Budapest, Hungary

[†]Institute for Data Science, Cloud Computing and IT Security, Furtwangen, Germany

Abstract—As mobile networks continue to grow, enhancing security, reducing latency, and preserving user privacy are key challenges, especially in next-generation networks. An important approach is to bring authentication and access control mechanisms closer to the network edge. However, current methods often result in high delays and computational load, which is problematic for devices with limited resources. This paper addresses this issue by proposing a verifiable and decentralized end to end authentication and access control framework, named VITA. The framework aims to reduce latency and processing overhead when establishing secure communication with external service providers. VITA uses blockchain technology to move parts of the authentication and access control process away from the central network, which reduces bottlenecks and improves scalability. VITA offers a secure, scalable, and lightweight solution suitable for resource-constrained IoT environments in Beyond 5G (B5G) and 6G networks. The results analysis showed that VITA reduces the authentication latency by 80.1% compared to the traditional approach. Furthermore, subsequent token-based authentication and access reduced the latency by about 96.1%.

Index Terms—B5G, 6G, Trust Management, Authentication, Access Control, Privacy Preserving framework.

I. INTRODUCTION

The rapid development of fifth-generation mobile networks has enabled the large-scale deployment of Internet of Things (IoT) devices. As we move toward Beyond 5G (B5G) networks, the requirements for handling massive data, supporting a vast number of devices, ensuring low latency, and delivering reliable services on demand become more critical [1]. These demands introduce new challenges [2], particularly in terms of authentication security and system scalability.

In B5G networks, key challenges can be grouped into four major areas: scalability, sustainability, trustworthiness, and digital inclusion [3]. Among these, trustworthiness is vital, as it ensures that only authenticated nodes are allowed to participate in the network. With billions of interconnected devices, it is essential to maintain strong authentication and access control mechanisms that can secure communication and protect against unauthorized access [4], [5].

Current 5G authentication protocols such as 5G-AKA and EAP-AKA depend on centralized network functions like the Authentication Server Function (AUSF) and Unified Data Management (UDM). These centralized systems can become

bottlenecks under heavy load. Furthermore, formal analyses have revealed potential vulnerabilities in these protocols when subject to real-world adversarial conditions [6].

To address these limitations, this paper explores a decentralized approach for authentication and access control by utilizing blockchain technology. The goal is to reduce reliance on the core network, eliminate central bottlenecks, and offer a scalable and secure solution suitable for resource-constrained IoT environments. The main contributions of this paper are as follows:

- Propose VITA, an Authentication and Access Control (AAC) framework that reduces the necessity and dependency on the core network during an End to End (E2E) trust establishment between the User Equipment (UE) and the service provider.
- Deploying the proposed framework in 5G testbed and providing a security and performance analysis that demonstrated the VITA's security, efficiency and applicability.

The remainder of this paper is structured as follows: Section II discusses related work. The 5G authentication has been explained in Section III. Section IV presents the proposed VITA framework. Section V provides performance and security evaluations, and further analysis and insights. Finally, Section VI concludes the paper.

II. RELATED WORK

Authentication and access control in B5G networks are critical for maintaining trust and protecting against unauthorized access [5]. The shift from centralized architectures to decentralized mechanisms is actively explored, particularly using blockchain [7] and edge computing [8] technologies. Basin et al. [6] formally analyzed the 5G authentication protocol and identified several vulnerabilities in adversarial threat models, such as compromised serving networks and time synchronization issues. Their work highlighted the risks associated with centralized authentication architectures.

Haddad et al. [9] proposed a framework for mutual authentication and key agreements using blockchain. Their approach does not require hardware changes and minimizes communication costs. Experimental evaluation showed reduced latency and improved scalability in IoT environments. Feng et al. [10] developed a cross-domain authentication protocol for 5G Internet of Drones using threshold signature aggregation.

The protocol ensures authentication across multiple domains with minimal overhead, though real-world performance results are not reported. Goswami and Choudhury [11] designed a blockchain protocol for 5G-enabled IoT environments. Their contribution was distributing credential management across trusted nodes to reduce authentication delay. Simulations showed improvements in latency and trust establishment.

Putra et al. [12] proposed a blockchain-based trust management framework. It uses smart contracts to automate trust evidence collection and score calculation. Their contribution was the transparent trust process stored in an immutable ledger, ensuring auditability and data integrity. Garba et al. [13] proposed LightCert4IoTs, a lightweight certificate management system using smart contracts and local registration authorities (LRA). IoT devices self-sign certificates which are validated at the edge. The novelty is in minimizing PKI complexity for constrained devices. However, the integration with full 5G network functionality was not realized. Aanandaram and Deepalakshmi [14] introduced the DIA-BC protocol, where each IoT device is assigned a blockchain-based digital identity. The novelty lies in eliminating dependency on centralized authorities using public key infrastructure (PKI) integrated with blockchain. Although promising, the protocol remains limited in practical deployment.

Fei et al. [15] introduced a decentralized framework for secure E2E communications in large-scale heterogeneous networks. Their framework combines blockchain, trusted execution environments (TEE) [16], and a privacy-preserving mutual authentication protocol. While technically rich, integration into diverse hardware remains a challenge. Goswami et al. [17] developed blockchain-enabled handover authentication and identity protection mechanisms. The unique feature is seamless identity retention during handovers. Experimental results showed reduced latency and improved user privacy. Choi et al. [18] presented a trust management framework for drone systems using physical unclonable functions (PUFs). The novelty lies in enhancing physical-layer security while maintaining lightweight operations. Their framework is particularly adapted to drones but has not yet been generalized to other IoT domains.

The current research shows a strong trend towards decentralized authentication using blockchain to address security, latency, and scalability issues in 5G and B5G networks. However, most proposals in the literature remain theoretical, with limited real-world implementation or integrationability into the 5G core network. Furthermore, the complexity of integrating technologies such as Trusted Execution Environment (TEE) within various devices raises concerns about compatibility and accessibility, potentially limiting the widespread adoption of such frameworks across different network infrastructures.

VITA contributes to providing a fully operational, standards-aligned framework that eliminates any centralized control using real-time blockchain events, uses pseudonym-based identity, smart contracts, and token-based access control to deliver decentralized, privacy-preserving authentication for IoT devices in 5G networks.

III. 5G AUTHENTICATION

According to the 3GPP TS 23.501 standard [19], the current fifth generation hierarchy consists of the user plane, access plane, core network, and data network, including external nodes such as IoT service providers. User devices connect to data networks through access and core networks, facilitating communication with service providers.

The authentication processes [19] involve several Network Functions (NFs) within the core network. The NFs operate as independent, modular functions that communicate using service-based interfaces. Each of them performs specific tasks, such as managing user sessions, handling authentication, or routing data. They are usually deployed in cloud environments. Most NFs reside in the core, and some NFs such as User Plane Function (UPF) can be closer to the edge. Among the main NF engaged in the authentication and access control process are Access and Mobility Management Function (AMF), AUSF and UDM. After receiving the UE request, the AMF initiates the authentication by communicating with the AUSF, which verifies the UE's credentials in conjunction with the UDM.

The authentication and access control process effectively manages the network through NFs in the core, ensuring security and reliability. However, when applied to end-to-end communication, it may introduce challenges such as increased delays. This is because authentication processes involve multiple steps and interactions between different NFs in the core as the requests must traverse the network to the core and back, potentially negatively affecting the performance of latency-sensitive applications. A UE on the network initiates a connection by first transmitting its concealed identifier Subscription Concealed Identifier (SUCI) to AMF. The AMF, acting as the initial contact NF, forwards this concealed identifier to the AUSF. The AUSF then communicates with the UDM to retrieve the necessary authentication parameters. Upon successful verification, the AUSF informs the AMF, which finalizes the initial registration and subsequently grants the UE access to the network.

Following the initial registration, the UE requests the establishment of a Protocol Data Unit (PDU) session to access data services. The AMF forwards this request to the Session Management Function (SMF), which then will interact with the Policy Control Function (PCF) and consults the UDM to enforce policy and subscription parameters. Subsequently, the SMF selects an appropriate UPF and configures it to route the UE's data traffic to the desired Data Network (DN). This process can introduce latency depending on the network configuration and the physical distance between NFs. Distributing the trust management process to be performed closer to the network edge can significantly reduce this latency and improve security by localizing traffic and minimizing exposure. To address this, VITA distributes the authentication and access control process to be closer to the end nodes, reducing the need for frequent interactions with the core network. The framework aims to minimize round-trip communications and distributes the process tasks more efficiently.

IV. VITA: THE PROPOSED FRAMEWORK

VITA is a hybrid solution that integrates blockchain technology into the existing 5G network architecture to provide decentralized authentication and access control for IoT devices. The framework has been built on the standard 5G core network architecture and is designed to maintain compatibility with existing 5G infrastructure. The combination of blockchain characteristics such as immutability and transparency provides a decentralized trust management mechanism for IoT. In the following sections, the system model, network model, and technical architecture of the proposed framework are explained in detail.

A. System Model

The VITA framework models the authentication and authorization process as a secure, distributed interaction among six key components: the UE, Next Generation Node B (gNB), the 5G Core, Service Provider, the Blockchain, and the Bridge. Each UE is cryptographically assigned a *pseudonym* to ensure privacy while interacting with other network components. The pseudonym functions as an anonymous on-chain identity used in authentication transactions.

a) *Pseudonym Generation*: Each UE is assigned a long-term identifier known as the Subscription Permanent Identifier (SUPI). Upon successful registration with the 5G core, the SUPI is used to generate a privacy-preserving pseudonym. The pseudonym is computed using the Keccak256 cryptographic hash function [20] applied over the concatenation of the SUPI, a time window (e.g., 12 hours), and a salt value:

$$pseudonym = H(SUPI || TimeWindow || Salt) \quad (1)$$

The output is a fixed-length string that represents the unique UE identity on the blockchain. This pseudonym, along with a hashed access policy and an expiration timestamp, is stored on-chain by invoking a smart contract function.

b) *Token-Based Access Control*: Once the UE is authenticated through its on-chain pseudonym, the service provider issues a digitally signed token that is bound to the authenticated pseudonym and its permissions. The token is used for subsequent access requests without re-querying the blockchain.

c) *Smart Contract Logic*: A permissioned Ethereum-compatible blockchain is used to record and manage the pseudonyms and service provider registrations. The smart contract logic enforces the verification process, including pseudonym validation, expiry check, and access policy compliance.

B. Network Model

VITA is designed to operate within the standard 5G network topology, extended with decentralized components for identity and trust management as illustrated in Figure 1. The network model involves the following entities:

- **UE**: An IoT device intending to join the network and access services.

- **gNB**: Acts as an intermediate node in the access layer that forwards UE registration requests to the core and enabling authentication communication.
- **Core Network**: The network that includes main NFs such as AMF and AUSF. It handles the UE's initial registration and pseudonym issuance.
- **Service Provider**: Offers services to authenticated UEs and validates access tokens using cached or on-chain data.
- **Blockchain**: A permissioned Ethereum ledger that stores pseudonyms, access control policies, and service provider metadata.
- **Bridge**: Connects the 5G core to the blockchain, listens to authentication events from the AMF, and writes authenticated identities to the blockchain.

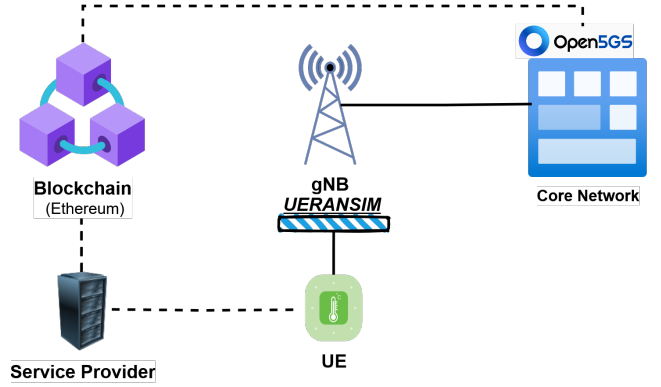


Fig. 1. Main Components and Actors in the VITA Framework

C. Architecture

Figure 2 illustrates the complete operational flow of the VITA framework. The system proceeds in three phases: UE Registration, Token Issuance, and Subsequent Authentication. Algorithm 1 outlines the main authentication procedure.

Algorithm 1 VITA Blockchain-Based Authentication

- 1: **Input**: UE registers via gNB to Core Network
- 2: Core authenticates UE; AMF logs are captured by Bridge
- 3: Bridge generates pseudonym and records it on blockchain
- 4: UE requests service access from Service Provider
- 5: Provider sends challenge; UE signs with wallet private key
- 6: Smart contract verifies pseudonym, validity, and access scope
- 7: **if** verification successful **then**
- 8: Service Provider issues token to UE
- 9: **else**
- 10: Access denied
- 11: **end if**
- 12: UE uses token for future requests; token verified locally

Below, the three phases of VITA and their main components are described in detail.

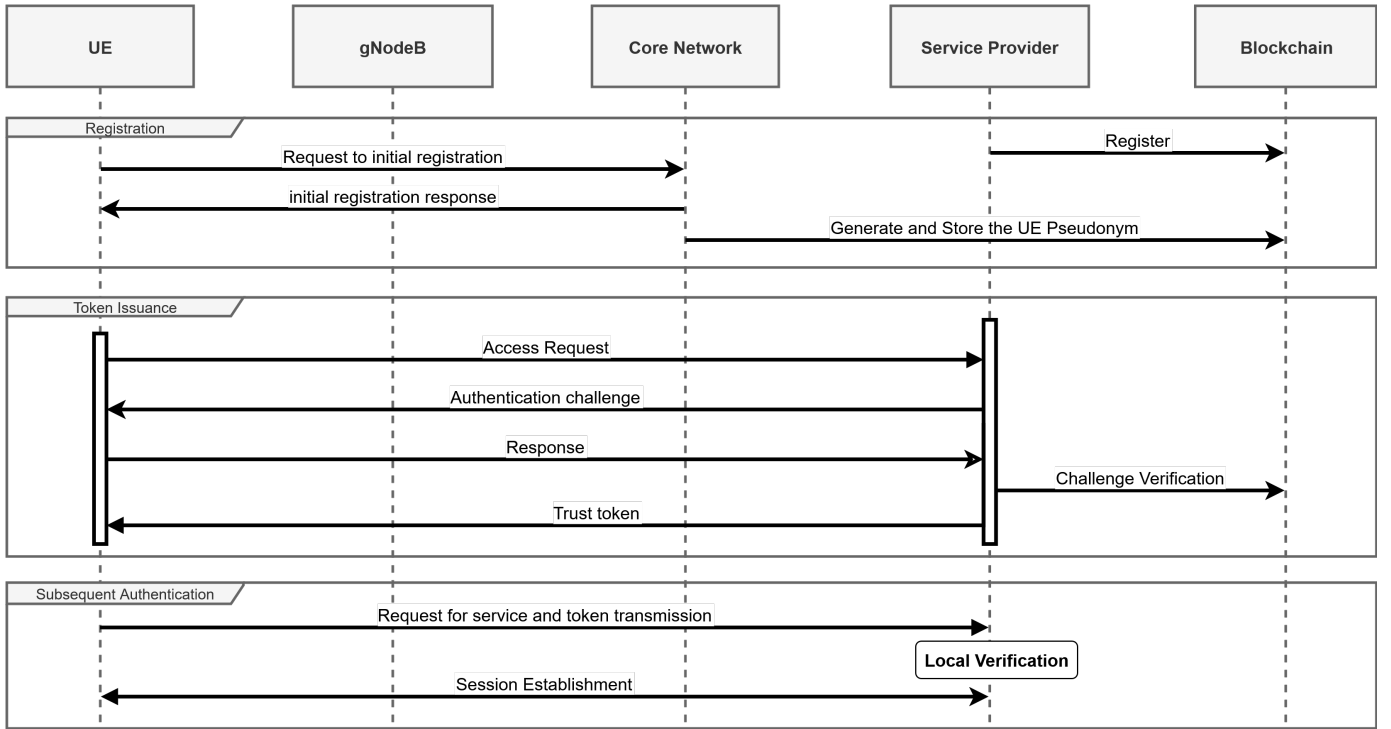


Fig. 2. Architecture and Workflow of VITA Authentication and Access Control

1) *UE Registration*: The UE sends a registration request to the gNB, which is then forwarded to the AMF within the core network. The AMF initiates the authentication and security procedure using standard 5G protocols. Meanwhile, the Bridge listens to any registration logs that are generated by the AMF. It then extracts the required UE information and computes the pseudonym using the SUPI, current time window, and a random salt. This pseudonym, along with a hash of the access policy and expiration timestamp, is then written to the blockchain via a transaction to the smart contract. The core network finalizes the registration by sending back a confirmation to the UE.

2) *Token Issuance*: When the UE attempts to access a service provider during the validity window of the pseudonym, the following procedure is executed:

- The service provider generates a random cryptographic challenge and sends it to the UE.
- The UE signs the challenge using its blockchain wallet's private key.
- The signed challenge and the UE's pseudonym are submitted to the smart contract function `verify_Authentication`.
- The smart contract checks if:
 - 1) The pseudonym exists and is valid.
 - 2) The pseudonym is within its expiration time.
 - 3) The access policy hash matches the required service scope.
- Upon successful verification, the service provider issues a verifiable token and sends it to the UE via HTTPS.

3) *Subsequent Authentication*: For repeated access, the UE presents the previously issued token. The service provider performs a local validation by verifying:

- The integrity and authenticity of the token.
- The expiration timestamp.
- The consistency with cached pseudonym and access policy information.

To improve performance, the service provider maintains an in-memory token cache with automatic eviction for expired tokens. This approach allows a fast and blockchain-independent authentication, which fits the nature of latency-sensitive IoT environments.

V. EXPERIMENTATION AND ANALYSIS

A. Implementation Setup

To evaluate the proposed framework in a controlled setting, a local testbed was deployed incorporating all core components of the architecture. A permissioned Ethereum blockchain was used, utilizing Foundry in a private setup, ensuring full control over the consensus and transaction mechanisms. Foundry has been utilized due to its lightweight, developer-friendly framework, which allowed efficient local testing and fast deployment of smart contracts. Additionally, a permissioned Ethereum has been used to ensure access control and low-latency consensus among trusted entities, such as telecom operators. This setup suits IoT environments where performance, reliability, and controlled participation are essential, unlike public blockchains that suffer from higher latency and unpredictable transaction fees.

The UE and gNB have been implemented using UER-ANSIM. The 5G core network functions, specifically AMF, AUSF, and UPF were implemented using Open5GS platform. These components were configured to operate in a simplified environment, mimicking a real 5G deployment without external noise.

The bridge module acts as the link between the AMF and the blockchain. It continuously listens and captures authentication logs from the AMF. This integration ensured near real-time synchronization between the 5G core events and the blockchain records. All test components ran on machines with the following specifications:

- Intel Core i7 CPU @ 1.8GHz, 16 GB RAM
- Ubuntu 24.04 LTS OS
- VMWare machines with negligible background traffic

To ensure statistical reliability and minimize transient effects, each scenario was repeated 100 times. The system was kept under consistent load and minimal latency conditions, isolating protocol-level performance from environmental interference. In future work, evaluations under varying network conditions can be also considered and explored to further validate the robustness of the proposed framework.

B. Performance Metrics

The following metrics were used to assess the authentication performance of the VITA framework:

- **Authentication Latency:** Measured from the initiation of authentication to the response received, across three defined scenarios, traditional 5G core authentication, initial blockchain-assisted authentication, and subsequent token-based authentication.
- **Standard Deviation:** Indicates the variability and stability of authentication response times. A lower value signifies more consistent performance.
- **Percentile Metrics:** Specifically the 95th and 99th percentile values, which help in understanding worst-case latency scenarios that is critical for latency-sensitive IoT applications.
- **CDF Distribution:** The Cumulative Distribution Function (CDF) plots provide a holistic view of latency spread and reveal the consistency and tail behavior of the authentication process under different scenarios.

C. Performance Analysis

To analyze the performance improvements introduced by VITA, the authentication process was evaluated across three scenarios:

- 1) **Traditional 5G Core Authentication:** In this case, the UE authenticates directly with the 5G core (via AMF and AUSF) using the standard 5G-AKA protocol.
- 2) **Blockchain-assisted Initial Authentication:** This represents the first-time authentication using the VITA framework, where the pseudonym and authentication token are verified through a smart contract on the blockchain.

- 3) **Subsequent Authentication using Token:** In this scenario, the UE presents the previously issued authentication token directly to the service provider. Since both the 5G core and blockchain are bypassed, only the token validation is performed.

Each scenario was executed 100 times, and the latency values (minimum, maximum, and average) were recorded. Table I shows the comparison across the three scenarios.

TABLE I
AUTHENTICATION LATENCY COMPARISON

Scenario	Minimum Latency (ms)	Maximum Latency (ms)	Average Latency (ms)
Traditional 5G Core Authentication	262	2793	427.69
Initial Authentication (Blockchain-assisted)	76	113	85.07
Subsequent Authentication (Token-based)	14	23	16.49

It is clear from the results that VITA significantly improves authentication performance. In the initial authentication phase in which the blockchain is used for pseudonym and token verification, the average latency is reduced by approximately 80.1% compared to the traditional 5G core method. The maximum latency also remained tightly bounded under 120 ms, which is favorable for time-sensitive applications.

In the subsequent authentication phase, where the already issued token is validated directly, the latency is further reduced by 96.1%. This phase eliminates the need for core or blockchain interaction, resulting in an ultra-lightweight and low-latency process ideal for repetitive device authentications in IoT networks. To better understand the latency behavior across the 100 authentication attempts, a CDF analysis was performed. The results are illustrated in Figure 3.

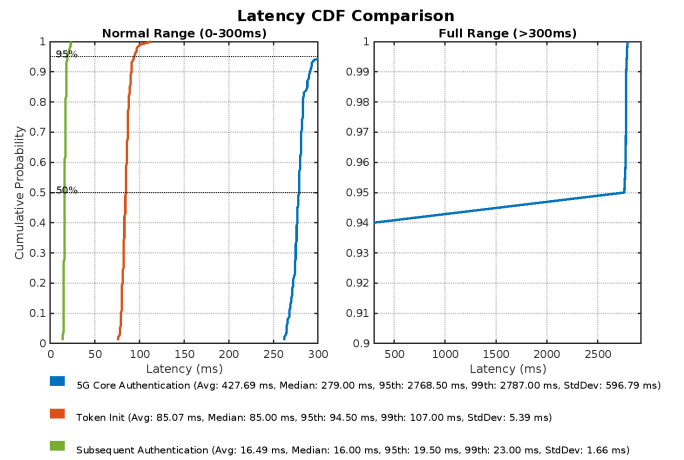


Fig. 3. Latency CDF Comparison between the 3 Scenarios

The CDF plot of the traditional 5G authentication reveals a wide and skewed distribution. The minimum latency is 262

ms, with the median at 279 ms. However, extreme outliers push the 95th percentile latency to 2768.5 ms and the 99th percentile to 2787.0 ms. These values reflect long-tail behavior due to backend processing delays, queuing, or random core-side overhead. The standard deviation of 596.79 ms further indicates unstable performance.

In contrast, the latency distribution of VITA's initial authentication is significantly narrower. All attempts fall within the range of 76 ms to 113 ms, with an average of 85.07 ms. The 95th percentile is just 94.50 ms, and the standard deviation is 5.39 ms. This shows a highly consistent authentication behavior, where most requests are completed under 100 ms, fulfilling the low-latency requirements of many industrial IoT systems.

Subsequent authentication shows even greater stability. The latency of this token based process consistently falls between 14 ms and 23 ms, with an average of 16.49 ms. The standard deviation is 1.66 ms, and over 99% of the authentication attempts are completed below the 23 ms mark. This makes VITA suitable for dense IoT environments where frequent and ultra-fast authentication is required. The framework not only minimizes the average latency significantly across all authentication phases, but also ensures highly predictable performance with minimal variability.

D. Security Analysis

The security of the VITA framework is analyzed under a defined threat model, and supported by discussions on privacy, replay protection, and forward security.

a) Threat Model and Assumptions: A semi-honest 5G core network is considered, which executes the protocol but may attempt to infer sensitive information from intercepted messages. The blockchain is assumed permissioned and governed by trusted entities, ensuring integrity and controlled access. Devices and service providers may utilize tamper-resistant hardware modules to securely store cryptographic keys, preventing key leakage.

b) Privacy and Unlinkability: Let S denote the SUPI, t the discrete time window index, and r a secret random salt known only to the core network. The pseudonym P is computed as:

$$P = H(S \parallel t \parallel r)$$

where $H(\cdot)$ is a collision-resistant cryptographic hash function, and $\parallel$ denotes concatenation.

This construction ensures that for each time window t , a unique pseudonym P is generated, unlinkable to previous pseudonyms due to the changing t and secret r . The adversary, observing P , cannot invert H to recover S , nor correlate P values across different t values without r . Hence, privacy is preserved as:

$$\Pr[\text{Link}(P_{t_1}, P_{t_2})] \approx \frac{1}{|R|}$$

where $|R|$ is the salt space size, making linking infeasible.

c) Replay Attack Resistance: Authentication tokens are valid only within their associated time window t . The system stores a cache $\mathcal{C}$ of pseudonyms P with expiration timestamps τ_{exp} . On receiving a token request with pseudonym P' , the system verifies:

$$P' \notin \mathcal{C} \quad \wedge \quad \text{current time} < \tau_{exp}$$

If this condition fails, the token will be rejected as a possible replay attack. Since tokens and pseudonyms expire after time Δt , replay attempts using stale tokens have zero probability of acceptance.

d) Forward Security: Even if an adversary compromises the secret salt r or tokens at time t , the pseudonyms of the previous time windows remain secure due to the one-way nature of H and the temporal ordering. Formally, having the knowledge of r and P_t does not help in computing P_{t-1} or recovering S because:

$$P_{t-1} = H(S \parallel (t-1) \parallel r)$$

and H is preimage resistant. This temporal unlinkability provides forward secrecy, preventing previous identity reveal.

e) Access Control: The smart contract on the blockchain acts as an oracle for authentication token validity. Let $V(P, T)$ denote the verification function where P is the pseudonym and T the presented token. Access is granted if and only if:

$$V(P, T) = \text{True}$$

where V verifies that T was issued for P within the valid time window and has not been revoked or used. This decentralized enforcement ensures that no entity can bypass or spoof authentication.

f) Bridge Security: The bridge module is an interface between the core and the blockchain, and is a critical element in the VITA framework. It operates as a listener and transaction handler. From a security perspective, the bridge component is protected under the assumptions of a secure execution environment and secure key storage. To further secure this vital component, the following measures can be implemented.

To prevent key leakage, all cryptographic material such as Ethereum private keys used to sign blockchain transactions can be stored in isolated secure containers such as hardware-backed keystore or OS-level secret management. Access will be restricted through file permission hardening, and keys are never exposed in memory in raw format. To protect against Denial of Service (DoS) attacks, the bridge listener can be implemented with a rate-limiting mechanism and request queuing, preventing event flooding. Moreover, since the bridge operates asynchronously with the core, short bursts of events are buffered and signed transactions are serialized using nonces to avoid collisions.

Regarding log tampering, logs from the AMF need to be parsed directly from its runtime output, or from a direct interface from the AMF. Only verified and structured authentication events are passed into the blockchain. Each interaction is signed and timestamped before submission, ensuring data

integrity. The immutability of the blockchain further protects against retroactive manipulation.

E. Technical Insights

In the following, the main technical insights of VITA have been stated:

- **Privacy-Preserving Identities:** Pseudonyms anonymize UE identities while ensuring traceability through hash-based computation.
- **Smart Contracts:** Ensure decentralized and verifiable authentication without relying on a central managing authority.
- **Offline Verification:** Use of signed tokens reduces blockchain interaction and latency.
- **Compatibility:** VITA operates within existing 5G architecture without hardware changes.
- **Efficiency:** In-memory caching and time-based pseudonym expiration reduce gas cost and computational overhead.

VI. CONCLUSION

This paper proposes an authentication and access control framework (VITA) by utilizing the blockchain technology into authentication processes of the core network. It improves security, decrease authentication latency, and enable scalable IoT deployments. The framework evaluated by designing and implementing its major components, including a smart contract for device authentication, a service provider backend for challenge-response authentication and token management, and a UE client for running device simulation scenarios. The performance analysis results showed that VITA performs significantly better than 5G core network authentication in terms of latency. In addition, different test scenarios have been designed to evaluate the performance of the framework. The results of these tests have shown that the framework can handle the edge cases securely and efficiently.

Several issues remain as future research directions. The blockchain component runs in a permissioned environment among multiple trusted parties. The future work can investigate more decentralized or hybrid blockchain designs, such as federated trust models, to further enhance the decentralization of the system, and at the same time, maintain the high performance and security of the framework. Additionally, the evaluation of VITA can be extended by testing it under various network conditions to understand its performance in diverse environments better. Formal security verification of the VITA framework needs to be performed. Formal methods can be used to prove the correctness, privacy, and robustness of the system against various attacks. Specifically, the security of the bridge component can be further studied by addressing potential threats. Furthermore, the VITA scalability can be studied to support a larger number of devices and more complex IoT applications, making it more practical for widespread use in beyond 5G networks.

REFERENCES

- [1] S. Birtane, M. Al-Naday, F. Paolucci, R. A. Bakar, V. Lefebvre, V. Passas, S. Kalafatidis, A. Lalas, A. Drosou, E. M. de Oca, *et al.*, "Footprint-optimized orchestration and management of secure complex services over 6g continuum," in *2024 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 383–388, IEEE, 2024.
- [2] R. Patil, Z. Tian, M. Gurusamy, and J. McCloud, "5g core network control plane: Network security challenges and solution requirements," *Computer Communications*, vol. 229, p. 107982, 2025.
- [3] C. G. Brinton, M. Chiang, K. T. Kim, D. J. Love, M. Beesley, M. Repeta, J. Roese, P. Beming, E. Ekudden, C. Li, *et al.*, "Key focus areas and enabling technologies for 6g," *IEEE Communications Magazine*, vol. 63, no. 3, pp. 84–91, 2025.
- [4] V. H. La, W. Mallouli, M. D. Nguyen, E. M. de Oca, A. Cavalli, P. Vörös, K. Kecskeméti, M. Alshawki, S. Laki, A. Lalas, *et al.*, "Enhancing iot security in 6g networks: Ai-based intrusion detection, penetration testing, and blockchain-based trust management (work-in-progress paper)," in *IFIP International Internet of Things Conference*, pp. 53–67, Springer, 2024.
- [5] P. Scalise, M. Hempel, and H. Sharif, "A survey of 5g core network user identity protections, concerns, and proposed enhancements for future 6g technologies," *Future Internet*, vol. 17, no. 4, p. 142, 2025.
- [6] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18*, (New York, NY, USA), p. 1383–1396, Association for Computing Machinery, 2018.
- [7] D. C. G. Valadares, A. Perkusich, A. F. Martins, M. B. Alshawki, and C. Seline, "Privacy-preserving blockchain technologies," *Sensors*, vol. 23, no. 16, p. 7172, 2023.
- [8] T. Nguyen, H. Nguyen, and T. N. Gia, "Exploring the integration of edge computing and blockchain iot: Principles, architectures, security, and applications," *Journal of Network and Computer Applications*, vol. 226, p. 103884, 2024.
- [9] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based authentication for 5g networks," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 189–194, 2020.
- [10] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, 2022.
- [11] B. Goswami and H. Choudhury, "A Blockchain-Based authentication scheme for 5G-Enabled IoT," *Journal of Network and Systems Management*, vol. 30, 7 2022.
- [12] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Toward blockchain-based trust and reputation management for trustworthy 6g networks," *IEEE Network*, vol. 36, no. 4, pp. 112–119, 2022.
- [13] A. Garba, D. Khoury, P. Balian, S. Haddad, J. Sayah, Z. Chen, Z. Guan, H. Hamdan, J. Charafeddine, and K. Al-Mutib, "Lightcert4iots: Blockchain-based lightweight certificates authentication for iot applications," *IEEE Access*, vol. 11, pp. 28370–28383, 2023.
- [14] V. Aanandaram and P. Deepalakshmi, "Blockchain-based digital identity for secure authentication of iot devices in 5g networks," in *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, pp. 1–6, 2024.
- [15] S. Fei, Z. Yan, H. Xie, and G. Liu, "Sec-e2e: End-to-end communication security in ls-hetnets based on blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 1, pp. 761–778, 2023.
- [16] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *2015 IEEE Trustcom/Big-DataSE/ISPA*, vol. 1, pp. 57–64, IEEE, 2015.
- [17] B. Goswami and H. Choudhury, "A secure and fast handover authentication scheme for 5G-Enabled IoT using blockchain technology," *Wireless Personal Communications*, vol. 138, pp. 2155–2181, 10 2024.
- [18] J. Choi, S. Son, D. Kwon, and Y. Park, "A puf-based secure authentication and key agreement scheme for the internet of drones," *Sensors*, vol. 25, no. 3, p. 982, 2025.
- [19] B. 3GPP, "Security architecture and procedures for 5g system," 2020.
- [20] P. Prajapati, P. Shah, R. Shah, and D. Shah, "Comparative study on hash algorithms: Keccak, md, ripemd, and sha variants," in *World Conference on Information Systems for Business Management*, pp. 51–59, Springer, 2025.