Preprints.org

Article

Not peer-reviewed version

5G-DAuth: Decentralized Privacy-Preserving Service Authorization for 5G Network Functions

Rui Ma , Mingjun Wang * , Zheng Yan , Haiguang Wang , Tieyan Li

Posted Date: 11 December 2025

doi: 10.20944/preprints202512.1017.v1

Keywords: 5G; service-based architecture (SBA); network functions; blockchain; authentication and authorization; TEE

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

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

Article

5G-DAuth: Decentralized Privacy-Preserving Service Authorization for 5G Network Functions

Rui Ma [1], Mingjun Wang [1,*], Zheng Yan [1,2], Haiguang Wang [3] and Tieyan Li [3]

[1] School of Cyber Engineering, Xidian University, Xi'an, 710126, China
[2] State Key Lab of Integrated Services Networks, Xidian University, Xi'an, 710126, China
[3] Shield Lab., Singapore Research Center, Huawei Technologies, Singapore
* Correspondence: mjwang@xidian.edu.cn

Abstract

The 5G network adopts a cloud-native, service-based architecture (SBA) that enables support for diverse services via virtualized Network Functions (NFs). A key advantage of this architecture is its decoupling of the control plane and user plane, which enhances network flexibility and scalability. However, the reliance on virtualized implementations and cloud processing also expands the network's attack surface. For example, the centralized Network Repository Function (NRF) inherently faces the risk of single points of failure. Addressing these gaps requires a resilient security architecture that builds on the existing 5G security framework; yet, current research on security and privacy management for network function services remains relatively limited. To fill this research gap, this paper proposes 5G-DAuth: a decentralized security management scheme for NF services in 5G networks. 5G-DAuth is built on a consortium blockchain and integrates a trusted off-chain Trusted Execution Environment (TEE) pool. The consortium blockchain forms the foundation of a decentralized cross-domain security management platform for NF services, enabling automated registration, authentication, authorization, and access control for NFs. This design directly resolves the single-point failure risk associated with the centralized NRF. To ensure the confidentiality and integrity of service data, the off-chain TEE pool is specifically designed to support smart contract execution and secure service data storage. Additionally, we enhance access tokens using digital signature to achieve fine-grained access control for service authorization while protecting against man-in-the-middle (MITM) attacks and replay attacks during service access. We validate the security of 5G-DAuth through two complementary approaches: informal security analysis and formal verification via a dedicated verification tool. Experimental results further demonstrate that 5G-DAuth delivers high performance across different service management operations, with strong performance in terms of latency and throughput.

Keywords: 5G; service-based architecture (SBA); network functions; blockchain; authentication and authorization; TEE

1. Introduction

The 5th Generation Mobile Network (5G) offers a stable, fast, reliable, and secure foundational network for digital information transformation across various domains. By integrating innovative technologies such as Software-Defined Network (SDN), Network Function Virtualization (NFV), and Cloud-Native, 5G achieves high flexibility with deployment customization and scalability [1]. It demonstrates unprecedented capabilities in high-speed data transmission, low-latency communication, and massive device connectivity, thereby driving innovations and developments in applications such as the Internet of things (IoT), industrial Internet, smart cities, augmented reality, and virtual reality.

The 5G core network (5GC) is designed based on a "cloud-native" Service-based Architecture (SBA). In 5G SBA core network, Network Elements (NEs) evolve into software-based, modular Network

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

Functions (NFs) composed of multiple microservices. NFs communicate with each other via Service-based Interfaces (SBIs), combined in a bus-like topology. Each NF supports providing services to other NFs, enhancing load balance, fault tolerance, scalability, and maintainability of the 5GC [2].

However, while the 5GC adopts SBA to enhance network capacity and service quality, it also exposes a large attack surface compared to past networks, inevitably facing many new security and privacy challenges [3]. First, the centralized management of NFs presents drawbacks such as single points of failure and performance bottlenecks. The centralized Network Repository Function (NRF) in the 5GC is responsible for the registration, updating, deregistration, and authorization of NFs, carrying a significant communication load. If the NRF is broken through, the service interaction of the entire core network is greatly affected. Second, during the service authorization process, there are vulnerabilities in access control and identity authentication. Attackers can impersonate NF service consumers, hijack access tokens, and then carry out replay attacks and MITM attacks, achieving unauthorized access to services and malicious service invocation. Third, insufficient privacy protection measures for NFs could lead to such risks as core network service and resource leakage, exposure of network topology, and even theft of user-sensitive data.

Current research on the security of the 5GC mainly focuses on the security of key 5G technologies and improvements in UE authentication and key agreement [4][5]. However, research on NF management and service authorization security is relatively scarce. Issues such as the single point of failure of NRF, cross-domain service authorization security, and NF privacy protection urgently need to be addressed. The security and reliability of the 5GC are fundamental to ensuring the stable operation of 5G network services.

To address the security and privacy issues in 5G NF services management, in this paper, we propose 5G-DAuth, a decentralized secure and trustworthy NF service management scheme for 5G networks. 5G-DAuth offers trusted registration, authentication, authorization, and access control for cross-domain NF services sharing, built on a blockchain and an off-chain TEE-based security management platform. 5G-DAuth leverages the consortium blockchain to build a cross-domain authorization network among 5G public land mobile networks (PLMNs), and use smart contracts for NF management and service authorization. The computational tasks of smart contracts are offloaded to off-chain TEEs based on Intel SGX, achieving secure and efficient cross-domain NF service authorization and access control while supporting NF data privacy protection. Our contributions can be summarized as follows:

- We propose 5G-DAuth, a cross-domain 5G NF service authorization scheme based on a consortium blockchain and off-chain TEE. Our scheme constructs the consortium blockchain for NF communication between multiple PLMNs, utilizing smart contracts to provide NF management and service authorization, thereby addressing the single point of failure of NRF.
- We design an off-chain TEE based on Intel SGX to reduce block synchronization waiting time, enhance the computational efficiency of smart contracts, and ensure security and privacy for both smart contracts and on-chain data.
- We conduct serious security analysis and performance evaluation on 5G-DAuth to demonstrate that it meets security and privacy protection requirements while offering certain performance advantages.

The rest of this paper is organized as follows. Section II reviews related works with comparison. Section III presents the system model and security model of 5G-DAuth. Section IV describes the details of the 5G-DAuth design. Section V provides security analysis and performance evaluation. Finally, Section VI concludes the whole paper.

2. Related Work

In this section, we review related work on service authorization in 5GC, including access token-based and identity-based schemes.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

2.1. Token-Based Service Authorization and Access Control

The 3GPP standard specifies that 5G SBA use the OAuth 2.0 protocol for authorization and access control of NF services[6]. The OAuth 2.0-based service authorization mechanism contains three roles, Network Function Service Consumer (cNF), Network Function Service Producer (pNF), and Authorization Server (NRF), and uses a client credential model to provide service access tokens for cNF. The access token is based on JSON Web Token (JWT) and uses a digital signature or message authentication code to provide integrity protection. After obtaining the access token generated by the NRF, the cNF carries the token to initiate a service request to the pNF. Upon receiving the service access request from the cNF, the pNF uses the NRF's public key to verify the access token, comparing the service authorization information declared in the token with the service request message from the cNF. If the verification is successful, the pNF provides a service response to the cNF. For OAuth 2.0, attackers could hijack tokens or impersonate service consumers to request services, carrying out replay attacks and MITM attacks. Moreover, there are no privacy protection measures during NF interactions, posing a risk of leakage of NF configuration information as well as service and resource data.

In the research and analysis of 5G access control mechanism, Akon et al. [7] have explored the security of the 5GC access control mechanism through formal analysis. The paper introduces a model-checking framework named 5GCVerif to assess potential security vulnerabilities in access control mechanisms based on OAuth 2.0. By constructing an abstract model to capture the nuances of the 5GC's access control mechanism and evaluating 55 security properties through the model-checking process, the detection framework was applied to the open-source 5GC project Free5GC. This application led to the discovery of five new security vulnerabilities, including an impersonation of service producer attack, token reuse attack, default privilege escalation attack, authorization bypass attack, and parameter misuse attack.

Zhang et al. [8] proposed a security protection mechanism for 5G network access tokens based on service APIs, named SETOKEN. This mechanism enhances the security of access tokens by granting CA certificates to trusted NRF within the core network, adding random factors and serial numbers to the access tokens, and distinguishing between initial and subsequent access tokens. This approach not only improves the security of access tokens but also optimizes token usage efficiency to prevent MITM and replay attacks. However, the scheme does not consider the potential single point of failure issue with the NRF as an authorization center and the privacy protection issues of NFs.

Zhu et al. [9] presented a security-enhanced scheme for NF service access in the 5GC based on business processes. To guard against issues such as NF identity impersonation, unauthorized service access, and replay attacks, this scheme incorporates a token identifier field bound to the business process into the access token and establishes an access token repository for global management of token identifiers. Additionally, it designs a mechanism for NF service producers to re-sign tokens and shares a token repository to enhance security. Although this scheme improves the security of service authorization, its efficiency is lower compared to the authorization mechanism based on OAuth 2.0. Moreover, the increase in shared token repository data also brings additional storage burdens and shares the same single point of failure issue with the NRF.

2.2. Identity-Based Service Authorization and Access Control

In the study of service authorization and access control for access users, Ferdi et al. [10] proposed a dynamic authorization framework to address service authorization and negotiation in 5G multi-tenant network slicing. This framework, building upon the basic service and static subscription configuration and authorization model of 3GPP, introduces the concepts of constrained services and negotiated services. Constrained services allow for standardized service definitions while maintaining the persistence of existing pre-configuration practices, and additionally provide the capability for dynamic authorization based on the context of service requests.

Kiyemba et al. [11] addressed the issue of federated identity management and network service access control in 5G networks and other heterogeneous networks by proposing a protocol for Network

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

Service Federated Identity (NS-FId). The protocol, designed on the 5G Service-Based Architecture (SBA), employs OAuth 2.0 as the authorization framework. It supports secure access to services from multiple service providers and provides users with single sign-on capabilities.

Luo et al. [12] proposed a composable multi-factor authentication and authorization scheme for 5G services. By introducing a hierarchical identity management framework, they constructed an authentication and session key agreement protocol based on three factors: biometrics, passwords, and smart cards. This protocol allows for flexible identity verification and an efficient authorization process that can be segmented or combined according to the security levels required by different services. In conjunction with the 5G Service-Based Architecture (SBA), they also proposed a service authorization process based on the three-factor authentication mechanism. NRF generates an access token based on the user's identity, session key, and smart card.

Table 1 compares related work with ours regarding the security requirements in terms of privacy preservation, access control security, resisting replay and MITM attacks, cross-domain, and preventing single points of failure. Through comparison, it is evident that most of the current 5G service authorization schemes are implemented based on the OAuth 2.0 protocol. Many of these schemes do not consider the single point of failure issue of the authorization server, lack research on service authorization in cross-domain scenarios, and fail to provide adequate privacy protection for 5G NF configuration and service data.

Table 1. Comparison of 5G-DAuth with existing schemes.

Security Requirement	[8]	[9]	[10]	[11]	[12]	5G-DAuth
PP	○	○	○	○	●	●
AC	●	●	●	●	●	●
RAR	●	●	○	○	●	●
MAR	●	●	○	○	●	●
CD	○	○	●	●	○	●
SPFP	○	○	○	○	○	●

[1] PP: Privacy Preservation; AC: Access Control; RAR: Replay Attack Resistant; MAR: MITM Attack Resistant; CD: Cross Domain Support; SPFP: Prevention of Single Point Failure. [2] ●: satisfy the security requirement; ○: do not satisfy the security requirement.

3. Problem Statements

In this section, we present the system model of 5G-DAuth, including four main modules, and define the security model. Table II lists the notations used in this paper.

3.1. System Model

The overall system model is shown in Figure 1. The system of 5G-DAuth consists of four main modules, i.e., the home Public Land Mobile Network (hPLMN), the visiting Public Land Mobile Network (vPLMN), the Consortium Blockchain (CBC) and the pool of Off-chain Trusted Execution Environment (Off-Chain TEE). The network mode of PLMN is based on a Service-based Architecture (SBA). Network Functions (NFs) register with the Network Registry Function (NRF). The hPLMN and the vPLMN connect to the consortium blockchain network through the NRF's bridge. The NRF acts as a blockchain client and initiates transactions with it. To facilitate mobile roaming, cross-domain service invocations are made between the NFs in the vPLMN and hPLMN. A Trusted TEE pool is established off the blockchain to provide an efficient and secure environment for computation and storage. The concrete functions of the main modules are described as follows:

- NF is the network function that provides various network services. Before it can offer services, the NF must first register with the NRF. NFs can be categorized as either Network Functions consumer (cNF) in a vPLMN or Network Functions provider (pNF) in hPLMN during a service invocation. To ensure that the invocation between different NFs is credible, the cNF requires

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

service authorization from the NRF and must adhere to the access control set by the pNF. NFs communicate with one another through Service-Based Interfaces defined within the core network.

- NRF handles registration and authorization requests from NFs, functioning as a client for the consortium blockchain. It initiates transactions and invokes smart contracts with the blockchain nodes. In 3GPP specifications [6], NRF serves as a central server for NF management. In the 5G-DAuth system, to reduce the risk of a single point of failure, most functions of the NRF are transferred to a consortium blockchain and smart contracts. The NRF operates as a blockchain client, initiating service requests and invoking the relevant smart contracts.
- The consortium blockchain is responsible for processing smart contract invocation requests related to the registration, management, and authorization of NRFs in PLMNs. It selects a group of Enclaves from the off-chain TEE pool to execute the corresponding smart contracts. Each PLMN can establish multiple nodes on the consortium blockchain. These nodes receive smart contract invocations from the NRFs and respond with the execution outcomes. A management smart contract, referred to as M, is deployed on the consortium blockchain to oversee the lifecycle of the Enclaves within the TEE pool. This contract M is responsible for creating the Enclaves for smart contract execution, instantiating the smart contracts, and logging the status of the Enclaves on the consortium blockchain. Any PLMN that connects to the consortium blockchain can access the on-chain ledger to view the status of enclaves and the smart contracts deployed within those enclaves. We design three essential contracts, namely the NF management contract, service authorization contract, and service subscription contract.
- The off-chain TEE pool selects an enclave as an Executor and initializes and executes smart contracts within the Executor. In the 5G-DAuth, TEE is deployed outside the consortium blockchain, while smart contracts are executed within the off-chain enclaves. By this design, 5G-DAuth provides a reliable and efficient computation and storage environment for smart contract and NF data. The Executor receives smart contract execution requests from the consortium blockchain nodes and executes the smart contract code within a protected memory area. This ensures the security of the smart contract code and prevents attackers from eavesdropping on and stealing data during code execution. The Enclaves utilize the sealing mechanism to encrypt and store data on the consortium blockchain and interact with the blockchain to achieve state synchronization. To ensure the availability of the off-chain TEE pool, we learn a resilience scheme from POSE [13]. Before executing a smart contract, two additional enclaves known as Monitors are chosen to oversee the executor's operational status. If the Executor does not return results within a specified time, the Monitors initiate an inquiry mechanism to question the executor or switch to another available Executor.

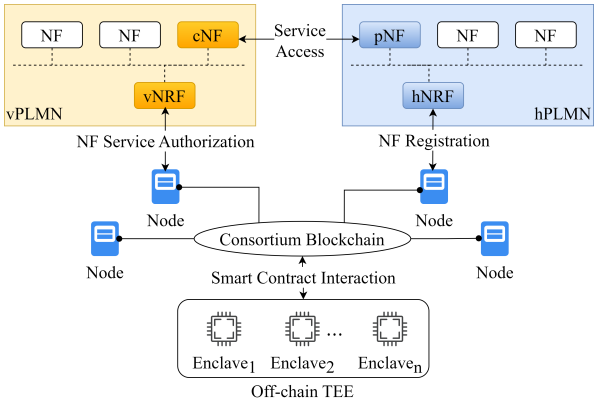

Figure 1. System Model of 5G-DAuth

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

3.2. Security Model

We analyze the security threats towards NF service authorization and cross-domain service access and propose corresponding security assumptions for each system module under the security architecture 5G system defined in 3GPP specification [14].

In the system, each NF, NRF, and consortium blockchain node is equipped with a digital certificate issued by a trusted CA. The communication links between NFs, as well as between NFs and NRFs, are protected by existing security protocols, e.g., TLS protocol. Cross-domain communications between NFs in different PLMNs are secured through the use of the Security Edge Protection Proxy (SEPP) [14] to ensure the safety of the hypertext transfer protocol (HTTP) signaling. The communication between NRF and the off-chain TEE during the invocation of smart contracts is secured for confidentiality and integrity using a session key sk, which is negotiated in the initialization phase between both parties. The admission mechanism of the consortium blockchain ensures that all nodes joining the network are authorized. Each node in the consortium blockchain is equipped with a certificate issued by the consortium's Certificate Authority (CA), which ensures its trustworthiness.

In this paper, we assume the TEE can protect programs executed in the enclaves, in line with other TEE-assisted blockchain proposals. Although recent research has revealed various potential security risks associated with SGX, such as side-channel attacks and cache attacks, there are appropriate technical strategies available to effectively mitigate these risks [15]. In 5G-DAuth, the enclave operating off-chain within the TEE undergoes remote authentication with the consortium blockchain during initialization to provide unforgeable cryptographic proof. The enclave ensures the trustworthy execution of NF management and service authorization smart contracts, safeguarding their operational state and data privacy from theft. Given that the TEE is deployed outside the consortium blockchain, a TEE execution pool is constructed with multiple Enclaves [13], i.e., an Excutor and multiple Monitors, to ensure the availability and robustness of the TEE. Additionally, the NF configuration information and PLMN's network topology are securely stored on the blockchain using TEE's data sealing mechanism, and only the same enclave can decrypt the data during the execution of smart contracts.

4. 5D-DAuth Design

In this section, we present a detailed description of 5G-DAuth. We first give a design overview and then introduce the key steps of 5G-DAuth, specifically system initialization, NF management, service authorization, and service access.

4.1. 5G-DAuth Overview

5G-DAuth is a decentralized network function service security management system that integrates consortium blockchain technology and off-chain TEEs within a 5G SBA core network. It leverages consortium blokchain and smart contract to construct a decentralized platform for cross-domain NF management and automatic service authorization and access control. Mobile operators or third-party service providers can deploy smart contracts on the blockchain to automate the processes of NF service registration, authentication, authorization, and access control. Additionally, 5G-DAuth maintains an off-chain TEE pool to execute these smart contracts and safeguard data off-chain. This approach ensures the confidentiality of NF profiles and policy information while reducing synchronization time and computational costs. With its well-thought-out design, 5G-DAuth eliminates the single point of failure associated with the NRF, protects the privacy of NF service information, and enhances the overall execution efficiency of the system.

4.2. System Setup

Consortium Blockchain Initialization: 5G-DAuth is composed of multiple PLMNs owned by different mobile operators. Each operator registers several nodes on a consortium blockchain. A subset of nodes invokes smart contracts, while others handle transaction packaging and block synchronization. Within each PLMN, an NRF is associated with one of the consortium blockchain nodes and responsible

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

for invocating smart contracts on the blockchain as an external client. During the initialization phase, each NRF generates a public-private key pair (PK_{NRF}, SK_{NRF}), which is used to sign smart contract transaction proposals and negotiate a session key with the associated consortium blockchain node. After the initialization of the consortium blockchain network, an on-chain smart contract M is deployed on the blockchain. M is responsible for creating off-chain enclaves and deploying NF management smart contracts. In the scenario of two PLMNs' cross-domain service invocation, the consortium blockchain establishes a specific channel between the associated blockchain nodes of PLMNS and creates a private ledger for this channel. The configuration and service authorization information of NFs are recorded in this ledger.

Enclave Initialization and Smart Contract Deployment: PLMN sends the enclave creation and smart contract deployment requests to the associated consortium blockchain node via the NRF. The request includes the code of a smart contract SC_{code} and its hash value $H(SC_{code})$, as well as the public key of the NRF PK_{NRF}. The consortium blockchain node invokes M to generate a $SCID$ for the smart contract, initialize an enclave (i.e., Executor) within the off-chain TEE, and deploy the code of the smart contract into the enclave. The Executor generates an enclave identifier EID and an attestation report ϕ, as well as a session key sk and a public-private key pair (PK_E, SK_E). After the enclave is initialized, it sends EID, ϕ, PK_E, and $Enc(sk, PK_{NRF})$ back to M. Subsequently, M stores the Enclave's EID, ϕ, PK_E, and the smart contract's $SCID$ and $H(SC_{code})$ in the consortium blockchain ledger. The consortium blockchain node sends EID, ϕ, PK_E, $SCID$, and $Enc(sk, PK_{NRF})$ to the NRF, enabling it to invoke the smart contract. The NRF subsequently decrypts the session key sk using its private key SK_{NRF} and uses sk to encrypt the messages between NRF and the enclave.

4.3. NF Management

In the 5G-DAuth system, the management of the NF life cycle is facilitated through smart contracts under the oversight of the NRF. The NRF invokes smart contracts to implement the registration, updating, and deregistration of NFs. Before providing and consuming services, an NF first registers to the NRF by submitting NF configuration information $NFProfile$. The $NFProfile$ is stored on the consortium blockchain, facilitating decentralized NF management and cross-domain NF service discovery. The detailed process of NF registration is illustrated in Figure 2 and described as follows:

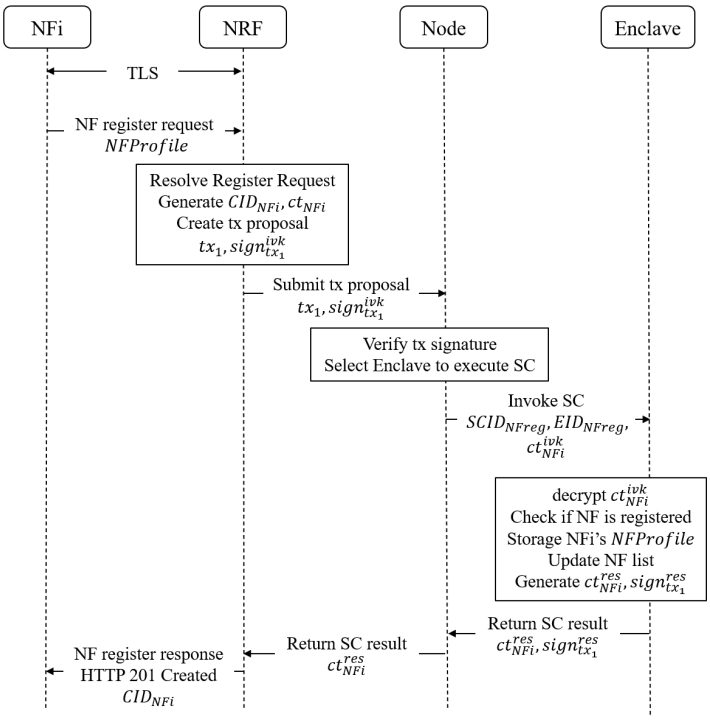

Figure 2. NF Registration

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

Step 1: NF sends registration request to NRF. Before initiating a registration request, a network function instance NF_i first engages in TLS mutual authentication with the NRF to establish a secure transport channel between NF_i and NRF. Subsequently, NF_i invokes the NRF's service API Nnrf_NFManagement/nf-instances/nfinstanceID with a PUT request. The registration request message from NF_i carries data that constitutes the configuration information $NFProfile$ of the NF instance. The $NFProfile$ includes both standard and optional configurations. The standard configurations are attributes that must be submitted upon NF instance registration, such as NF instance ID ID_{NF}, NF type $nfType$, NF status $nfStatus$, PLMN ID ID_{PLMN}, FQDN or IP address, NF service set $services$, and NF load information $nfLoad$, among others. Optional configurations are properties that are customized for specific NF functionalities, such as the GUAMI in the AMF or the SMF region ID in the UPF.

Step 2: NRF invokes smart contracts to blockchain nodes. Upon receiving registration information from NF, NRF further processes the NF instance information. Firstly, NRF conducts a hash operation on the instance ID of NF_i to generate a hidden ID to conceal the identity of the registered NF. Subsequently, NRF encrypts $NFProfile$ using the session key sk between NRF and Enclave to obtain $ct_{NF_i}^{ivk}$. Then, NRF constructs a transaction proposal $tx_1(SCID_{NFreg}, EID_{NFreg}, CID_{NF_i}, ct_{NF_i}^{ivk})$ for invoking the smart contract $SCID_{NFreg}$ for NF registration. Then, NRF signs the transaction with NRF's private key and sends the transaction proposal and transaction signature to the consortium blockchain nodes.

Step 3: Blockchain node invokes enclave to execute smart contract. Upon receiving the transaction proposal from NRF, consortium blockchain nodes first validate the signature $sign_{tx_1}^{ivk}$ using PK_{NRF}. Subsequently, they invoke the NF registration smart contract within Enclave based on $SCID_{NFreg}$ and EID_{NFreg}. The Enclave utilizes the session key sk to decrypt and obtain plaintext $NFProfile$, parses its attributes, and performs further processing. It retrieves the $nfType$ and ID_{PLMN} of the NF instance, encrypts $NFProfile$ using the Enclave's sealing key K_{seal}, initiates a write request to the consortium blockchain, and stores the key-value pair $(CID_{NF_i}, Enc(NFProfile, K_{seal}))$ in the consortium blockchain ledger. Additionally, a registered NF list for NF service discovery is maintained on the consortium blockchain. When a new NF is registered, a new entry is added to this list in the form of a key-value pair $(ID_{PLMN} : nfType, \{CID_{NF_1}, CID_{NF_2}, CID_{NF_i}\})$, encrypted using K_{seal} as well. Upon completion of the execution of the smart contract $SCID_{NFreg}$, the Enclave encrypts the execution result using sk to obtain $ct_{NF_i}^{res}$, signs it using SK_E to obtain $sign_{tx_1}^{res}$, and returns them to the consortium blockchain nodes.

Step 4: NF receives registration success response. The consortium blockchain nodes validate the signature of the ciphertext execution result using PK_E, return the ciphertext execution result to NRF, and perform transaction packaging and ledger synchronization between nodes. NRF decrypts the execution result using sk to obtain the registration status of NF_i, and then sends an HTTP 201 response to NF_i along with CID_{NF_i}, informing NF_i of the successful registration.

4.4. Service Authorization

When a cNF from vPLMN intends to access a service provided by a pNF in hPLMN, a service discovery and authorization request must be initiated for vNRF. The authorization operation is carried out by the smart contract $SCID_{auth}$, which is responsible for service discovery and authorization. Based on the cNF request, the smart contract $SCID_{auth}$ queries the target service access address and issues the corresponding authorization token. The service authorization process is illustrated in Figure 3.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

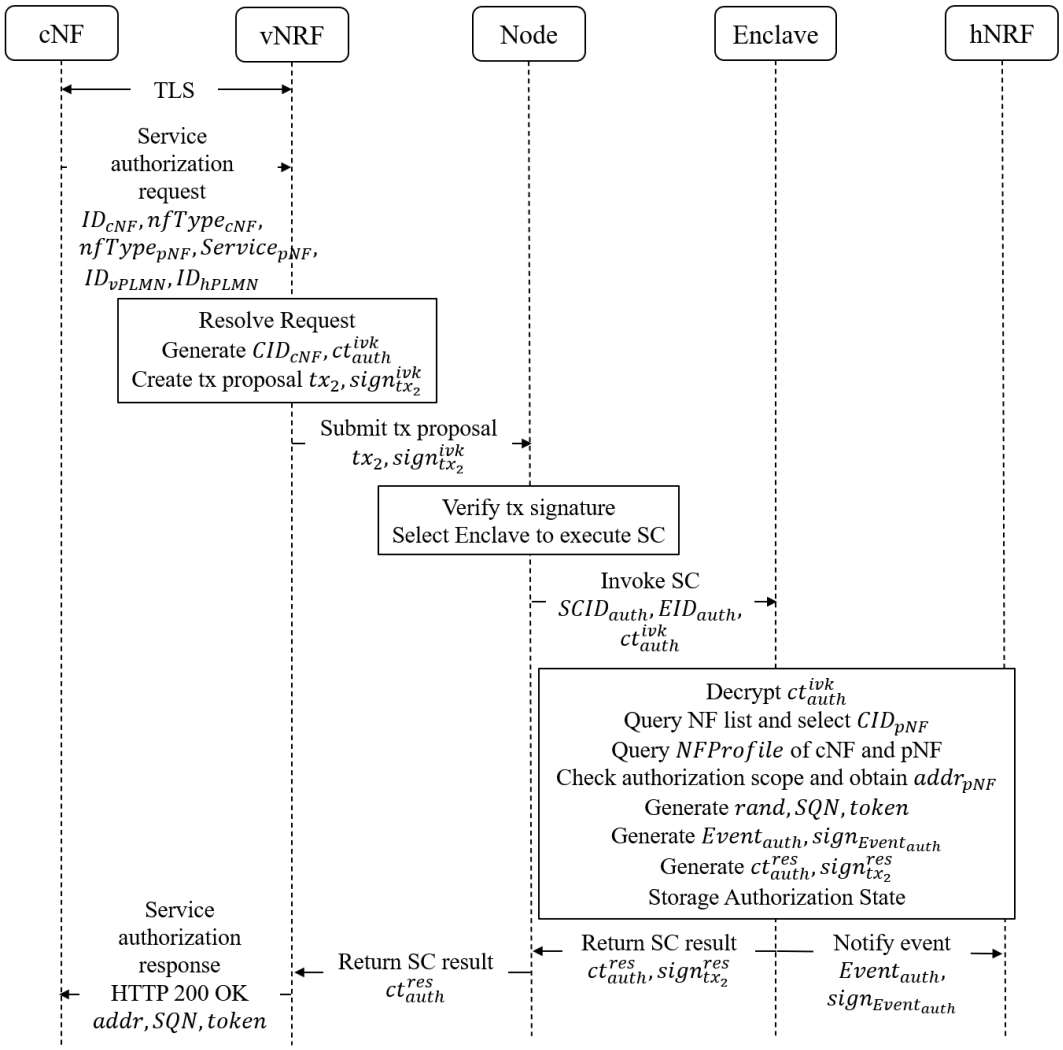

Figure 3. Service Authorization

Step 1: cNF initiates a service discovery and authorization request to vNRF. Firstly, cNF and vNRF establish a secure communication channel through TLS mutual authentication. Subsequently, cNF invokes the API Nnrf_AccessToken provided by vNRF, initiating a GET request. The request message includes the cNF instance ID, cNF type, vPLMN ID where cNF is located, target pNF type, target service type, and hPLMN ID where the pNF is located.

Step 2: vNRF initiates smart contract invocation to consortium blockchain nodes. Upon receiving the request from cNF, vNRF further processes the request. Firstly, it computes the CID_{cNF} for cNF, then encrypts the parameters of the service authorization request using the session key sk_{vNRF} between vNRF and Enclave to obtain ct_{auth}^{ivk}. Next, vNRF constructs a transaction proposal $tx_2(SCID_{auth}, EID_{auth}, CID_{cNF}, ct_{auth}^{ivk})$ for invoking the authorization smart contract $SCID_{auth}$. Then, vNRF signs the transaction and sends the transaction proposal along with the signature to the consortium blockchain nodes.

Step 3: Consortium blockchain nodes invoke Enclave to execute smart contract. Upon receiving the transaction proposal from vNRF, the consortium blockchain nodes validate the signature $sign_{tx_2}^{ivk}$ of the transaction proposal. Then, they invoke the smart contract $SCID_{auth}$ within Enclave EID_{auth}. Enclave utilizes the session key sk_{vNRF} to decrypt and obtain the service authorization request information from cNF. Firstly, Enclave searches for the registration status of cNF based on CID_{cNF}. If cNF is registered, the authorization process continues; otherwise, the authorization is aborted. Then, based on the pNF type $nfType_{pNF}$, Enclave queries the NF registration list to select a suitable pNF in hPLMN and retrieve its CID_{pNF}. Subsequently, the Enclave queries the $NFProfile$ of pNF on the

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

consortium blockchain based on CID_{pNF}. It extracts configuration information from $NFProfile$ including service name, service access address, service authorization scope, resource authorization scope, etc., and determines if the corresponding service can be provided to cNF within the authorization scope specified by the pNF. If cNF falls within the specified authorization scope of the pNF, Enclave generates a random number *rand* and a sequence number SQN, and creates an access token *token* for cNF. The attributes of the access token include the CID and type of cNF, the CID and type of pNF, the service provided by pNF, the expiration time of authorization, and the random number. The Enclave signs these attributes using the Enclave private key SK_E to obtain *token*. Upon completion of the smart contract execution, the Enclave sends the access token *token*, the target service access address $addr_{pNF}$, and the sequence number SQN as the contract execution result. These are encrypted and signed, then sent to the consortium blockchain nodes. The authorization information is sealed using K_{seal} and stored on the consortium blockchain. Utilizing the smart contract event listening mechanism, an event is predefined to apply for service authorization to pNF in hPLMN and generate an access token. When this event is triggered during the smart contract execution, encrypted event notifications and signatures are generated and sent to the hPLMN consortium blockchain nodes subscribed to this event.

Step 4: cNF receives authorization success response. The consortium blockchain nodes validate the signature of the ciphertext execution result using PK_E, then send the ciphertext execution result to vNRF and perform transaction packaging and ledger synchronization between nodes. vNRF decrypts the ciphertext execution result using the session key sk_{vNRF}, and sends the target service access address $addr_{pNF}$ and access token *token* to cNF. It informs cNF of the successful service authorization via an HTTP 200 response. Subsequently, cNF can initiate service access requests to pNF using the target service access address and access token.

4.5. Service Access

After obtaining service authorization, cNF can initiate service access requests to the target service address of pNF while carrying an access token. Upon successful validation of the request by pNF, the corresponding service can be provided. During the service authorization phase, hNRF retrieves event notifications from the alliance chain nodes. Using sk_{hNRF} to decrypt the notification, CID_{pNF}, CID_{cNF}, *rand*, and SQN are obtained. hNRF forwards CID_{pNF}, CID_{cNF}, *rand*, and SQN to pNF, which stores them for subsequent access token verification during cNF service access. The NF service access process is illustrated in Figure 4.

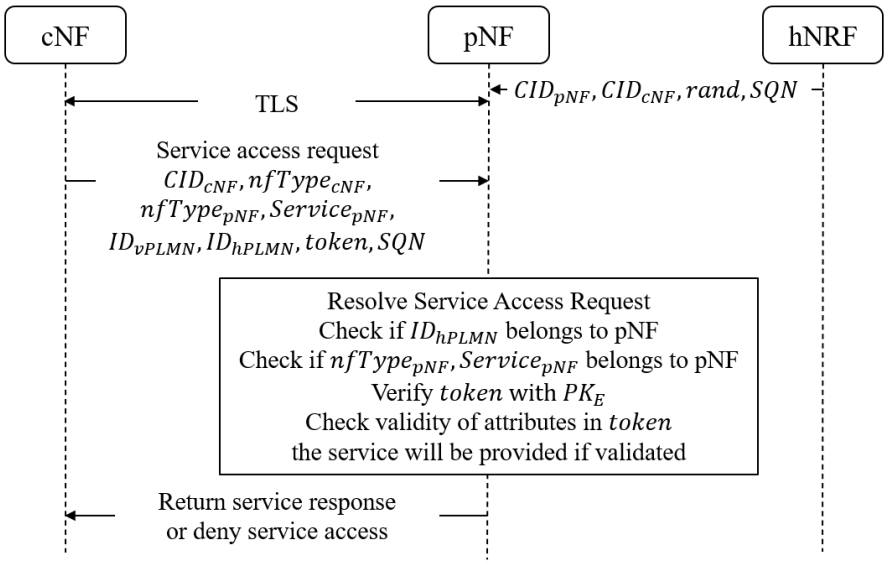

Figure 4. Service Access Control

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

Step 1: cNF initiates service access request to pNF. cNF and pNF first establish TLS mutual authentication for eligibility verification. cNF initiates a service access request to the target service address of pNF. The request message includes the CID of cNF, cNF type, pNF type, target service type, vPLMN ID where cNF is located, hPLMN ID where pNF is located, access token, sequence number, and specific parameters required for invoking the service.

Step 2: pNF validates the service access request. Upon receiving the service invocation request from cNF, pNF utilizes the Enclave public key PK_E to verify the token. It extracts the attributes from the token and compares them with the cNF request parameters. If the service requested by cNF is in an authorized state, the random number and sequence number correspond one-to-one, and the access token is within its validity period, pNF executes the service operation and returns the service response to cNF. Subsequently, pNF increments SQN.

Step 3: cNF obtains the service access result. pNF determines the legitimacy of cNF's service access based on the access token, then decides whether to execute the service or refuse it. Upon receiving the response message from pNF, if cNF receives a service response, it proceeds with subsequent operations and updates SQN. If cNF receives a refusal of service, it needs to request service authorization again.

5. Security and Performance Evaluation

This section provides a comprehensive security analysis, details the experiment design and implementation, and reports the performance evaluation results of f D5G-NFAu in terms of latency, throughput, CPU cost, and memory cost by comparing with a baseline.

5.1. Security Analysis

We analyze the security of 5G-DAuth from the perspective of security requirements and use AVISPA to formally verify the service authorization protocol.

Mutual Authentication: During the system initialization phase, public and private keys and digital certificates are generated for NF, NRF, and the consortium blockchain nodes. At the beginning of communication, the TLS protocol is used to authenticate the identities of both parties.

Confidentiality and Integrity: The communications between NFs and between NFs and NRF are both encrypted with a session key generated after identity authentication through the TLS protocol, ensuring secure and reliable transmission. For the communication between NRF and the consortium blockchain nodes, transaction proposals sent by NRF are signed with SK_{NRF}, allowing the consortium blockchain nodes to verify that the transactions originated from the correct sender. The smart contract invocation information sent by NRF is encrypted using the session key sk negotiated during the Enclave initialization.

Privacy Protection: On the data privacy protection level, the data sealing function provided by SGX is used to achieve encrypted storage of NF configuration information and service authorization information in the consortium blockchain ledger, ensuring that only authenticated Enclaves can decrypt the data, thus preventing unauthorized access to NF data. On the identity privacy protection level, before registration, the pNF of hPLMN generates a concealed identity identifier CID through hNRF, ensuring that when the cNF of vPLMN accesses services and authorizations, it only obtains anonymized pNF information. This prevents attackers from reconstructing the network topology through enumeration or other means.

Access Control Security: During the service authorization phase, the smart contracts check the registration status of both cNF and pNF, verify cNF request information against the service provision scope of pNF, specify the authorization expiration time, sign the access token with the Enclave's private key SK_E, and encrypt the authorization information with K_{seal} for storage in the consortium blockchain ledger. This ensures strict permission control and traceability of authorization information for cNF service authorization. During the service access phase, cNF must provide an access token to request services, while pNF verifies the legitimacy of the service request using the cNF identity information and the access token. The token is verified with the Enclave's public key PK_E to retrieve the service

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

authorization scope, which is then compared with the cNF's service request information to prevent unauthorized access by cNF.

Resisting Replay and MITM Attacks: After cNF requests service authorization, it obtains an access token signed by the Enclave's private key, with a unique *rand* value added to the token to ensure its uniqueness. When cNF requests service access, it must carry the access token and synchronize *SQN* with pNF for each request, preventing attackers from intercepting and replaying messages to gain unauthorized access. Additionally, since the communication between NFs uses the TLS protocol and SEPP-based cross-PLMN signaling transmission, the authenticity of identities and communication security are ensured. This prevents attackers from decrypting or tampering with communication messages during NF service authorization and access processes, thereby mitigating MITM attacks.

Preventing Single Points of Failure: Leveraging the decentralized nature of the consortium blockchain, the NF management and service authorization functions of NRF are implemented via smart contracts on the consortium blockchain. This decentralization prevents service disruptions in NF registration or access token generation caused by NRF attacks or failures, thereby achieving decentralized cross-domain NF management and service authorization.

We utilize AVISPA for the formal analysis of the NF service authorization protocol [16]. The protocol is modeled based on the Dolev-Yao model, and the verification result confirms that the NF service authorization process meets the specified security requirements. The formal verification result is shown in Figure 5.

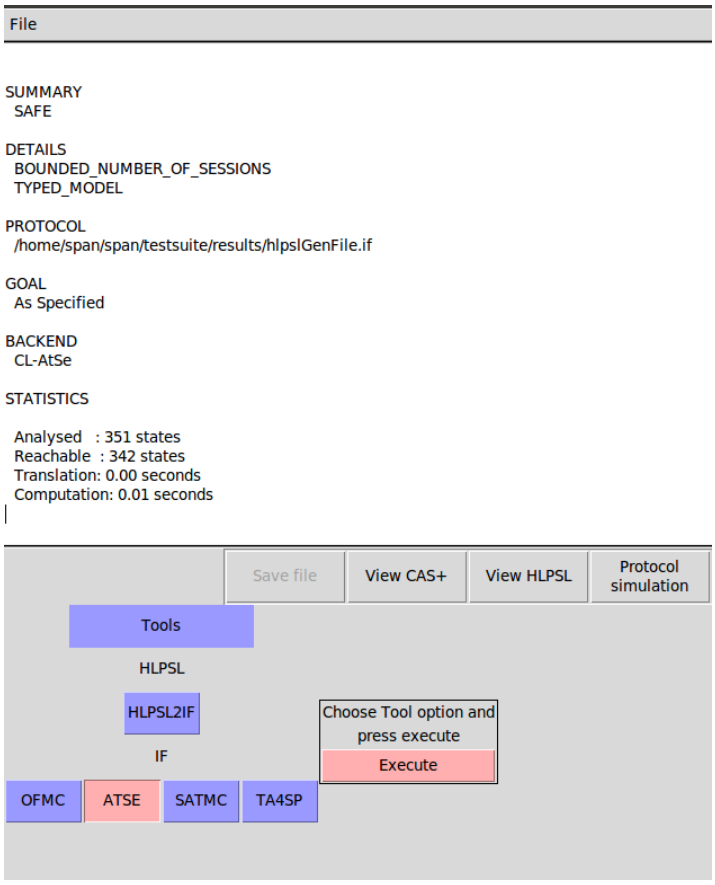

Figure 5. Formal Verification Result of AVISPA

5.2. Experimental Setup

Experiment Environment: 5G-DAuth utilizes the Hyperledger Fabric as the consortium blockchain, deploying relevant Enclaves using drivers and SDK provided by Intel SGX, and implementing the system on the Ubuntu Linux platform. Smart contracts for NF management and service authorization are developed using C++ and Intel SGX library functions. A Docker container is

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

employed to construct a 5G SBA core network simulation environment, simulating NF communication across PLMNs based on the inter-container communication mechanism of Docker containers. 5G SBA network functions are developed using Go and GIN framework, with each PLMN containing both cNF and pNF. Following the specifications of the 3GPP standard, message transmission between network functions is based on the HTTP/2 protocol, while service interfaces are provided in the form of RESTful Open API, with message data structured in JSON format. The digital signature algorithm utilized in the experiment is 256-bit ECDSA, the hashing algorithm is SHA-256, and the symmetric encryption algorithm used for Enclave sealing is 128-bit AES-GCM.

Baseline Method: Due to the lack of relevant research on blockchain-based cross-domain NF service authorization schemes in the literature and industry, we construct a baseline scheme for NF service authorization based on consortium blockchain and on-chain TEE for performance evaluation and comparison. The NF service authorization mechanism of the baseline is implemented on FPC[17]. By comparing with the baseline, we validate that applying off-chain smart contract TEE for cross-domain NF service authorization in 5G-DAuth has higher efficiency than the on-chain TEE solutions.

Evaluation Metrics: To evaluate the performance of the consortium blockchain with off-chain SGX for secure privacy protection, we compare 5G-DAuth with the on-chain TEE approach, mainly focusing on the latency and throughput of the consortium blockchain transactions. Additionally, we also compare 5G-DAuth with two other NF service authorization schemes based on access tokens proposed by Zhang [8] and Zhu [9]. The comparison includes the latency and resource utilization (CPU and memory), and security performance of access token generation and validation.

5.3. Experimental Results

This section details the prototype implementation of 5G-DAuth and presents its performance evaluation through experiments, focusing on the latency and throughput of various system operations, as well as the CPU and memory utilization under different volumes of token acquisition requests.

Figure 6 illustrates the variation trend of latency with the increase of NF number during the process of network function registration and service authorization. It can be observed from the figure that the latency gradually increases as the number of NFs increases. The numbers of read and write operations on the state data of the consortium blockchain ledger involved in the smart contracts for NF registration and service authorization, as well as the specific computations, vary. During the execution process of smart contracts, the state data that needs to be written is encrypted using the Enclave sealing key K_{seal}. In the NF registration smart contract, there is one read operation and two write operations on the state database. Firstly, it checks whether the NF instance has been registered based on $nfType$ and CID_{NF}. If the NF instance is not registered, it writes the NF configuration information into the state database and appends a CID_{NF} record to the NF registration list. In the service authorization smart contract execution process, there are two read operations and one write operation on the state database, as well as signature computations and event notification generation. Firstly, it searches the NF registration list based on $nfType$ and selects a suitable CID_{NF}. It retrieves pNF configuration information and generates an access token signed with the Enclave private key based on the authorization request parameters and the service authorization scope in the pNF configuration information. Then it stores the authorization information in the consortium blockchain ledger and generates an authorization event notification to hNRF.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

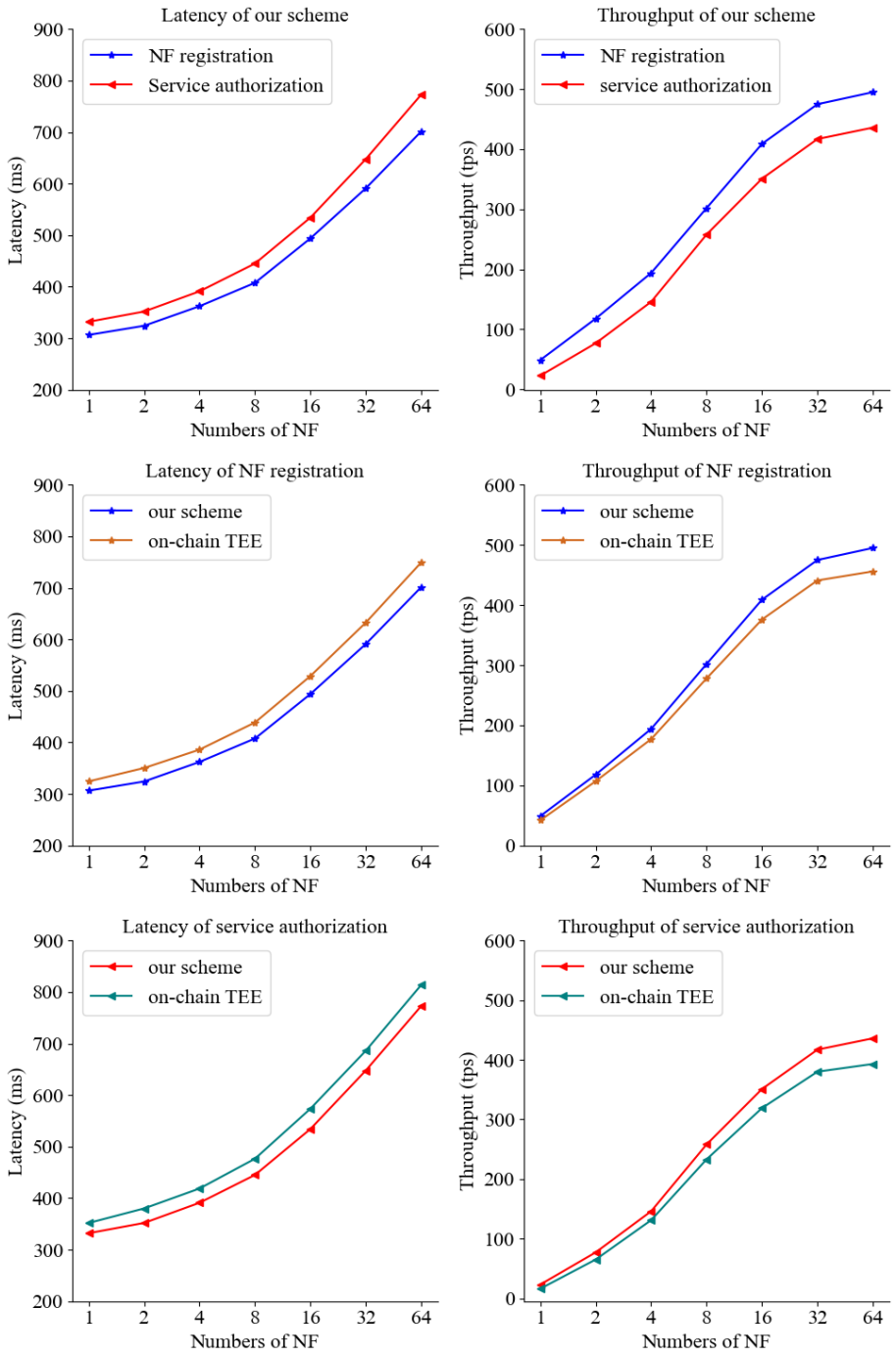

Figure 6. Latency and Throughput

5G-DAuth and the baseline with on-chain TEEs have the same processes of network function registration and service authorization. It can be observed that 5G-DAuth has a lower time overhead compared to the baseline. The main reason is that 5G-DAuth moves the execution of smart contracts to off-chain TEE, where they run within Enclaves. By providing authentication reports from the Enclaves and the signatures on the execution results of smart contracts, the endorsing nodes can trust the execution results of off-chain TEE. This reduces the time overhead caused by the need for multiple endorsing nodes to execute smart contracts, as in the baseline.

The variation trend of throughput with the increase of the number of NFs during the process of network function registration and service authorization is shown in Figure 6. As the number of NFs increases, the throughput also increases, and when the number of NFs reaches 16, the rate of increase

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

in throughput begins to slow down. The concurrent processing capacity of NRF, as well as the number of blockchain nodes and Enclaves, can impose limitations on throughput scalability. However, by increasing the number of concurrent connections supported by NRF and augmenting the number of blockchain nodes and Enclaves, this constraint can be mitigated, leading to enhanced throughput.

Specifically, we compare 5G-DAuth with two existing access token-based service authorization schemes proposed by Zhang [8] and Zhu [9]. The evaluation includes the token acquisition latency during the service authorization process, the token verification latency during service access, and the system CPU and memory utilization during service authorization execution. The results are shown in Figure 7.

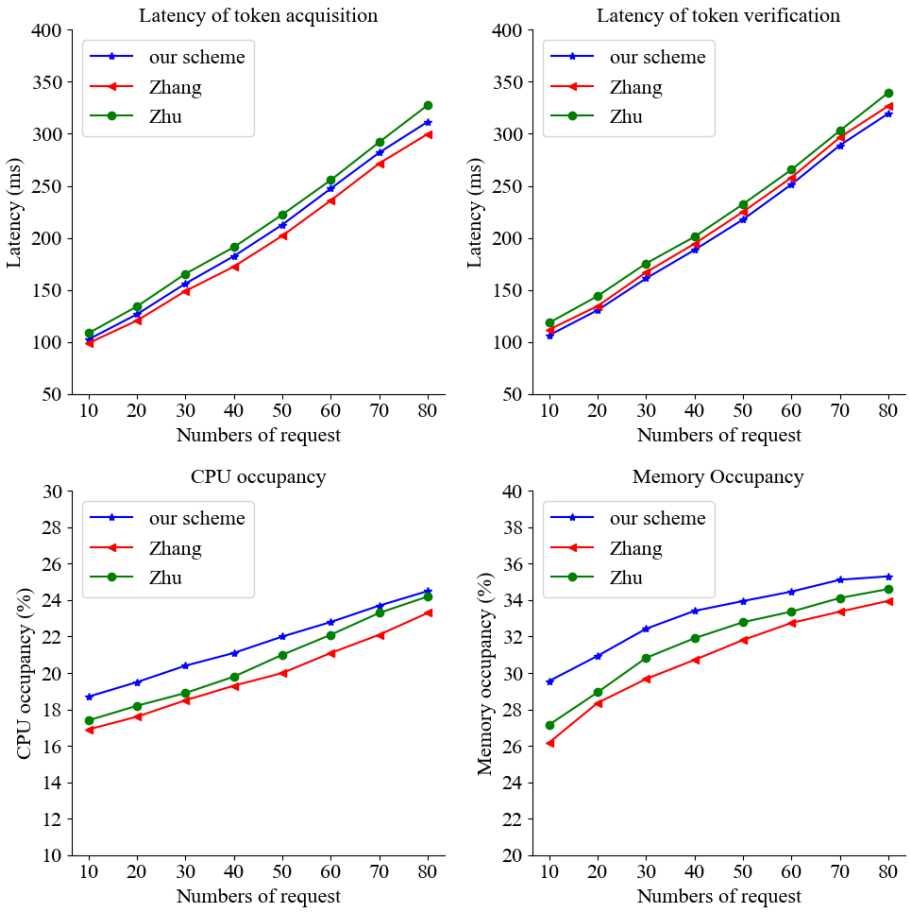

Figure 7. Comparison with Related Works Regarding Latency, CPU Cost, and Memory Cost

In 5G-DAuth, the token acquisition latency is lower than Zhu's scheme, mainly because Zhu's scheme introduces a business process table and a shared token repository. The NRF generates JSON web token (JWT) tokens after verifying whether the cNF service request complies with the business process relationship. Since 5G-DAuth utilizes Intel SGX to provide a trusted execution environment for token generation, there is a certain time overhead when decrypting the NF configuration information for privacy protection. Compared to Zhang's scheme, which generates access tokens in a less secure execution environment, the latency of 5G-DAuth is higher. The token verification process during service access is performed by the pNF in all three schemes. The token verification latency of 5G-DAuth is superior to both Zhang's and Zhu's schemes. Zhang's scheme requires two different hash function operations in addition to token verification, while Zhu's scheme requires token verification, storage, and re-signing upon the receipt of the token by the pNF. In contrast, 5G-DAuth utilizes smart contract event notifications to allow the pNF to obtain partial attributes of cNF service authorization in advance, enabling direct token verification upon the receipt of the access token.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

Regarding CPU and memory utilization, 5G-DAuth incurs additional CPU and memory consumption due to the context switching between the trusted and untrusted memory regions created by Intel SGX, as well as the memory swapping. While Intel SGX provides robust security and privacy protection capabilities, it comes with a performance cost to provide these security features. Despite the incurred performance overhead, experimental data indicates that the related overhead remains within the machine's normal operational range.

6. Conclusions

In this paper, we proposed a decentralized cross-domain service authorization scheme for 5G NFs, to address the security and privacy protection issues in 5G NF service authorization and access, as well as the single point of failure problem in NRF. We leveraged smart contracts to achieve NF management and service authorization. Through off-chain TEE, we ensured the trusted execution of smart contract codes and protected the privacy of NF configuration and service authorization data. Security analysis and performance evaluation show that 5G-DAuth not only meets security and privacy protection requirements but also achieves certain efficiency advantages.

Author Contributions: Conceptualization, Mingjun Wang and Rui Ma; methodology, Mingjun Wang, Rui Ma and Zheng Yan; software, Rui Ma; validation, Rui Ma; formal analysis,Rui Ma and Mingjun Wang; writing—original draft preparation, Rui Ma; writing—review and editing, Mingjun Wang and Zheng Yan; supervision, Haiguang Wang and Tieyan Li; project administration, Zheng Yan, Haiguang Wang and Tieyan Li; funding acquisition, Haiguang Wang and Tieyan Li. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by

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

Abbreviations

The following abbreviations are used in this manuscript:

5G	the fifth generation mobile networks
JWT	JSON Web Token
MEC	Mobile Edge Computing
MitM	Man-in-the-Middle Attack
NF	Network Function
NFV	Network Function Virtualization
NRF	Network Repository Function
PLMN	Public Land Mobile Networks
SBA	Service-based Architecture
SBI	ervice-based Interfaces
SDN	Software-Defined Network
TEE	Trusted Execution Environment

References

1. Shafi, M.; Molisch, A.F.; Smith, P.J.; Haustein, T.; Zhu, P.; De Silva, P.; Tufvesson, F.; Benjebbour, A.; Wunder, G. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. *IEEE Journal on Selected Areas in Communications* **2017**, *35*, 1201–1221.
2. Li, Y.; Huang, J.; Sun, Q.; Sun, T.; Wang, S. Cognitive Service Architecture for 6G Core Network. *IEEE Transactions on Industrial Informatics* **2021**, *17*, 7193–7203.
3. 3GPP TS 33.855. Study on security aspects of the 5G Service Based Architecture (SBA). Technical report, The 3rd Generation Partnership Project, 2024.
4. Kim, H. 5G core network security issues and attack classification from network protocol perspective. *Journal of Internet Services and Information Security (JISIS)* **2020**, *10*, 1–15.
5. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 3682–3722.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 December 2025 doi:10.20944/preprints202512.1017.v1

6. 3GPP TS 23.501. System Architecture for the 5G System (5GS). Technical report, The 3rd Generation Partnership Project, 2024.
7. Akon, M.; Yang, T.; Dong, Y.; Hussain, S.R. Formal Analysis of Access Control Mechanism of 5G Core Network. In Proceedings of the Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, 2023, CCS '23, p. 666–680.
8. Zhang, Y.; Liu, C.; Liu, S.; Pan, F. SETOKEN: A secure protection mechanism based on service API for 5G network access token. In Proceedings of the 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT), 2021, pp. 1139–1143.
9. Zhu, Y.; Liu, C.; You, W.; Zhang, Y.; Zhang, W. A Business Process-Based Security Enhancement Scheme for the Network Function Service Access Procedure in the 5G Core Network. *Electronics* **2023**, *12*.
10. Ferdi, S.; Shah, Y.; Kumar Choyi, V.; Brusilovsky, A. Dynamic Authorization for 5G Systems. In Proceedings of the 2018 IEEE Conference on Standards for Communications and Networking (CSCN), 2018, pp. 1–5.
11. Kiyemba Edris, E.K.; Aiash, M.; Loo, J.K.K. Network Service Federated Identity (NS- FId) Protocol for Service Authorization in 5G Network. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), 2020, pp. 128–135.
12. Luo, Y.; Li, H.; Ma, R.; Guo, Z. A Composable Multifactor Identity Authentication and Authorization Scheme for 5G Services. *Security and Communication Networks* **2021**, *2021*, 1–18.
13. Frassetto, T.; Jauernig, P.; Koisser, D.; Kretzler, D.; Schlosser, B.; Faust, S.; Sadeghi, A. POSE: Practical Off-chain Smart Contract Execution. In Proceedings of the 30th Annual Network and Distributed System Security Symposium, NDSS. The Internet Society, 2023.
14. 3GPP TS 33.501. Security Architecture and Procedures for 5G System. Technical report, The 3rd Generation Partnership Project, 2024.
15. Fei, S.; Yan, Z.; Ding, W.; Xie, H. Security Vulnerabilities of SGX and Countermeasures: A Survey. *ACM Comput. Surv.* **2021**, *54*.
16. Hassan, A.; Ishaq, I.; Minilla, J. Automated verification tools for cryptographic protocols. In Proceedings of the 2021 International Conference on Promising Electronic Technologies (ICPET). IEEE, 2021, pp. 58–65.
17. Brandenburger, M.; Cachin, C.; Kapitza, R.; Sorniotti, A. Trusted Computing Meets Blockchain: Rollback Attacks and a Solution for Hyperledger Fabric. In Proceedings of the 2019 38th Symposium on Reliable Distributed Systems (SRDS), 2019, pp. 324–32409.

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

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.