SGX-Enabled Encrypted Storage for Secure Management of 5G Authentication Data in Trusted Execution Environments

Adi Panca Saputra Iskandar[1,2], Changhyeon Woo[1], Linawati[2], Lely Meilina[2], Ilsun You[1]

[1]Kookmin University, Seoul, South Korea

[2]Udayana University, Bali, Indonesia

Received: November 29, 2025; Revised: January 07, 2026; Accepted: January 27, 2026; Published: February 05, 2026

Abstract

The fifth-generation (5G) core network, sensitive authentication data such as the Subscription Permanent Identifier (SUPI) and long-term cryptographic keys are centrally stored in the Unified Data Repository (UDR) to support primary authentication. Recent real-world incidents, including the 2025 SK Telecom (SKT) breach, demonstrate that compromise of core servers or databases can expose plaintext subscriber data even when transport-layer security is correctly deployed. This high- lights the need for strong data-at-rest protection and robust cryptographic key isolation within the 5G core. In this paper, we propose a storage-centric protection scheme that preserves the confidentiality and integrity of 5G authentication data even under authentication server compromise. Authentication records are encrypted before being stored in the UDR, with encryption and decryption operations in- voked through database triggers and executed inside an Intel Software Guard Extensions (SGX)-based Trusted Execution Environment (TEE). All cryptographic keys and sensitive operations are fully iso- lated within the enclave, preventing direct access from both the database and application layers. We implement the proposed design on the OpenAirInterface (OAI) 5G core using a MySQL-backed UDR, demonstrating its applicability to real-world and open-source 5G deployments. Performance evalua- tion over 10,000 end to end authentication procedures shows that the proposed approach introduces moderate CPU overhead, particularly during decryption-intensive operations, while incurring negli- gible memory overhead and minimal latency impact. These results indicate that SGX-based storage centric protection is a practical and effective mechanism for strengthening data at rest security in 5G core networks.

Keywords: 5G Core Security, Intel SGX, Trusted Execution Environment, Data-at-Rest Protection.

1 Introduction

The fifth-generation (5G) mobile communication system adopts a service-based architecture that enables flexible deployment, network slicing, and massive connectivity. Within the 5G core network, subscriber authentication and authorization rely on the secure management of highly sensitive credentials, includ- ing the Subscription Permanent Identifier (SUPI) and long-term cryptographic keys. These credentials are centrally stored in the Unified Data Repository (UDR) and accessed by network functions such as the User Data Management (UDM) during primary authentication, as specified in the 3GPP 5G security architecture [1]. Ensuring the confidentiality and integrity of authentication data is therefore critical to prevent subscriber identity exposure, impersonation, and large-scale service abuse. Early work on secure and ubiquitous networked systems has long emphasized the importance of protecting sensitive user data in distributed environments [2].

Although 5G standards provide strong protection for signaling and data in transit, recent incidents show that data at rest in the 5G core remains a major attack surface. In April 2025, a large-scale breach at a commercial 5G operator revealed that attackers with access to internal servers could extract plain- text authentication credentials from backend systems [3]. This demonstrates a key limitation of existing security assumptions: once the database or application layer is compromised, sensitive subscriber data stored in plaintext can be directly exposed, even when transport-layer protections remain intact. Such server-side compromises significantly expand the attack surface and enable downstream abuses such as subscriber tracking, identity correlation, and unauthorized network access. Current 5G security speci- fications primarily focus on mutual authentication, key agreement, and secure communication between the User Equipment (UE) and the core network [1], while protection of authentication data at rest in the UDR is largely left to implementation choices, often relying on database access control or disk-level encryption. Prior studies show that these mechanisms are insufficient against advanced adversaries or insider threats with privileged backend access [4, 5]. Once cryptographic keys or plaintext credentials escape a trusted boundary, the confidentiality guarantees of the authentication framework can be fun- damentally undermined. Moreover, recent work shows that authentication mechanisms themselves can be exploited at early stages, before full cryptographic protection is established, enabling large-scale denial-of-service and credential exposure attacks even in modern protocols such as EAP-TLS 1.3 [6].

To address this gap, hardware-based Trusted Execution Environments (TEEs) have emerged as a practical foundation for isolating sensitive computation and cryptographic key material. Intel Software Guard Extensions (SGX) provides enclave-based execution that protects code and data even in the pres- ence of a compromised operating system or hypervisor [7, 8]. By confining cryptographic operations and key management within a hardware-enforced enclave, SGX enables strong data-at-rest protection that remains effective under server compromise scenarios, particularly for database-centric components such as the UDR [9, 10]. In this work, we investigate SGX-based encrypted storage to harden authentication data management in the 5G core. We adopt a storage-centric protection model in which authentication data are encrypted before being written to the UDR, while all key generation, storage, encryption, and decryption operations are fully isolated inside an SGX enclave. As a result, plaintext credentials never reside in the database and cryptographic keys are never exposed to the database engine or application logic. Unlike prior conceptual proposals, this study presents a practical end-to-end implementation inte- grated into an open-source 5G core platform based on OpenAirInterface [11], demonstrating that strong data-at-rest protection can be achieved without prohibitive performance overhead.

Beyond protocol-level authentication, prior studies have explored broader security challenges in 5G core networks, including privacy risks, service-based architecture vulnerabilities, and emerging at- tack surfaces [12, 13]. Recent advances further highlight the growing role of intelligent and machine learning-based security mechanisms in defending against sophisticated attacks targeting 5G infrastruc- tures [14].

2 Motivation and Contributions

2.1 Motivation

Inside the 5G core network, subscriber authentication data are centrally stored in the Unified Data Repository (UDR), making it a critical trust anchor for primary authentication and service authoriza- tion. Although 3GPP specifications mandate strong cryptographic protection for signaling and mutual authentication, the security of authentication data at rest remains largely dependent on implementation- specific database protections. Recent large-scale breaches in commercial 5G deployments have demon- strated that compromise of backend servers can directly expose plaintext subscriber credentials, leading to severe privacy violations and downstream network abuse.

Conventional data-at-rest protection mechanisms, such as disk encryption and access control poli- cies, are insufficient against advanced adversaries and insider threats. Once attackers obtain administra- tive access to

the operating system or database engine, sensitive records and cryptographic keys can be extracted with minimal resistance. This threat model is particularly relevant in cloud-native 5G cores, where multi-tenant environments and complex operational workflows increase the risk of privileged ac- cess misuse [15]. Recent studies have strengthened 5G authentication security through protocol-level enhancements, including post-quantum cryptography and secure handover mechanisms [16, 17, 18]. However, these approaches primarily focus on signaling robustness and do not directly address the exposure of sensitive credentials stored within the UDR. While recent work has demonstrated the ben- efits of formal verification and protocol hardening for securing 5G handover and roaming procedures [19, 20], protection of authentication data at rest within the core network remains largely underexplored. As a result, even cryptographically robust authentication protocols remain vulnerable if their underlying credential storage is compromised.

Motivated by these limitations, we argue that effective protection of 5G authentication data must extend beyond secure communication and protocol design to include hardware-enforced protection of data at rest. Trusted Execution Environments (TEEs), such as Intel Software Guard Extensions (SGX), provide strong isolation for cryptographic operations and key material, remaining effective even under full server compromise scenarios. By integrating SGX-based encryption directly into the UDR storage workflow, plaintext authentication data can be prevented from ever leaving a protected enclave boundary.

2.2 Our Contributions

This work makes several key contributions to securing authentication data in 5G core networks. First, we propose a storage-centric security architecture that encrypts subscriber authentication data before they are stored in the Unified Data Repository (UDR), ensuring that plaintext credentials never reside in the database. Second, all cryptographic operations, including key generation, encryption, decryption, and integrity verification, are fully isolated within an Intel Software Guard Extensions (SGX) enclave, effectively eliminating direct access to cryptographic keys from both the database engine and appli- cation logic. Third, we present a practical and transparent integration of the proposed design into a real 5G core environment based on OpenAirInterface, leveraging UDR triggers, stored procedures, and user-defined functions to enforce encryption and decryption during normal authentication workflows. Fourth, we conduct an extensive end-to-end experimental evaluation covering 10,000 authentication attempts, systematically quantifying CPU utilization, memory consumption, and execution latency to demonstrate the practical feasibility of SGX-based encrypted storage. Finally, we show that the pro- posed approach preserves the confidentiality and integrity of subscriber authentication data even under database or application-layer compromise, significantly reducing the blast radius of potential security breaches in 5G core networks.

Table 1 provides a high-level comparison between existing approaches for protecting 5G authen- tication data and the proposed SGX-based storage-centric design. Conventional database encryption mechanisms protect data at rest but fail to isolate cryptographic keys from privileged system access, making them vulnerable under server compromise. Application-layer encryption partially improves key separation but still exposes sensitive material once the application or operating system is compromised. Protocol-level security mechanisms focus on protecting signaling messages and do not address the con- fidentiality of authentication data stored in the UDR. In contrast, the proposed SGX-based approach simultaneously provides strong data-at-rest protection, hardware-enforced key isolation, and resilience against server-side compromise, while maintaining a practical performance overhead suitable for real 5G core deployments.

Table 1. Comparison of Authentication Data Protection Approaches

Approach	Data-at-Rest Protection	Key Isolation	Server Compromise Resilience	Performance Impact
Database encryption	✓	×	×	Low
Application-layer encryption	✓	Partial	Partial	Medium
Protocol-level security	×	×	×	Low
Proposed SGX-based storage	✓	✓	✓	Low–Medium

3 System Architecture and Threat Model

3.1 System Architecture and Threat Model

The proposed system adopts a storage-centric protection architecture to secure subscriber authentication data in the 5G core network by integrating an Intel Software Guard Extensions (SGX)-based Trusted Execution Environment (TEE) directly into the Unified Data Repository (UDR) data path. As illustrated in Fig. 1 and Fig. 2, authentication data managed by the User Data Management (UDM), such as the Subscription Permanent Identifier (SUPI) and long-term subscription keys, are encrypted before being persisted and decrypted only inside a hardware-protected enclave during retrieval. The UDR is extended with database triggers, stored procedures, and user-defined functions (UDFs) that transparently invoke the SGX enclave on data insertion and access, ensuring that only ciphertext is stored at the database layer.

All cryptographic operations, including key generation, authenticated encryption, decryption, and integrity verification, are fully isolated within the enclave, preventing key exposure even under a com- promised operating system or privileged database access [7, 8]. Interaction between the UDR and the enclave is restricted to controlled UDF-based interfaces, minimizing the trusted computing base (TCB). This design builds upon prior work on shielded execution environments that enable secure execution of sensitive logic in untrusted systems [21], and follows established best practices for enclave development and deployment [22].

We consider a strong threat model in which an adversary can fully compromise the database and application layers of the 5G core, including the ability to access, modify, or exfiltrate UDR contents and execute arbitrary code at the operating system level. This model reflects realistic attack scenarios observed in recent large-scale 5G core breaches and insider threat incidents [3, 4]. Conventional pro- tections such as access control and disk encryption are therefore assumed insufficient. We assume that the hardware root of trust and the SGX enclave remain secure, while side-channel attacks against SGX are out of scope [23]. Network-level attacks are also excluded, as they are already addressed by existing 5G security mechanisms [1]. Under these assumptions, the primary security objective is to preserve the confidentiality and integrity of subscriber authentication data even when server-side components are compromised.

3.2 Diagram of Encryption and Decryption

Figure 1. Encryption flow for authentication data insertion in the UDR using an SGX enclave.

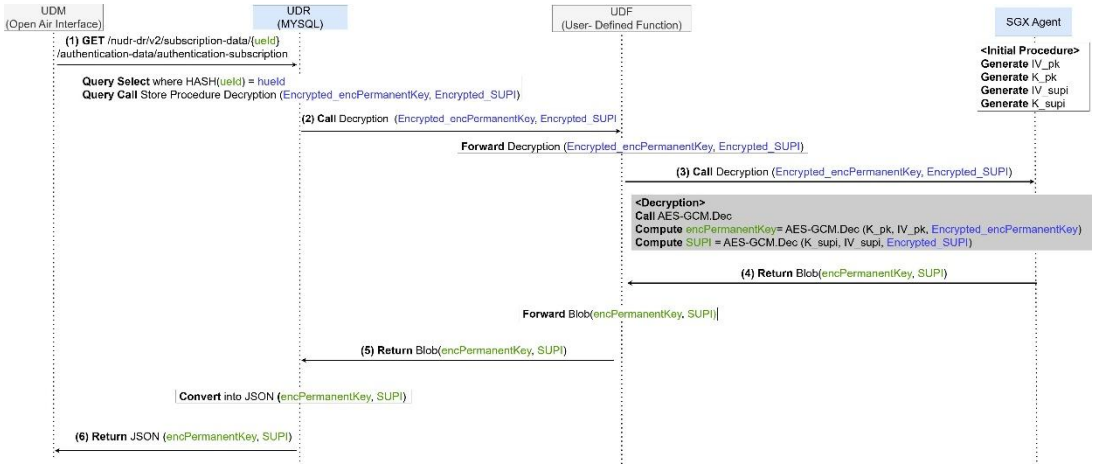

Figure 2. Decryption flow for retrieving authentication data from the UDR through an SGX enclave.

Figure 1 illustrates the encryption process applied when subscriber authentication data are inserted into the UDR. When the UDM submits authentication parameters, such as the SUPI and encrypted perma- nent key, a database trigger invokes a stored procedure within the UDR. This procedure forwards the sensitive fields to the SGX enclave via a user-defined function (UDF).

Inside the enclave, authenticated encryption is performed using the AES-GCM algorithm. Crypto- graphic keys and initialization vectors are generated and managed entirely within the enclave, ensuring that key material is never exposed outside the trusted boundary. The enclave outputs only ciphertext and authentication tags, which are returned to the UDR and stored in the authentication-related tables. As a result, plaintext authentication data never reside in the database at any point during the insertion process.

Figure 2 depicts the decryption process during authentication data retrieval. Upon a request from the UDM, the UDR locates the corresponding ciphertext records using a hashed user identifier. The encrypted data are

then passed to the SGX enclave through a UDF call.

Within the enclave, the ciphertext is decrypted and its integrity is verified using the internally man- aged cryptographic keys. Only after successful verification are the plaintext authentication parameters reconstructed and securely returned to the UDM. If integrity verification fails, the enclave rejects the re- quest and no plaintext is released. This design ensures that only validated and untampered authentication data are used in subsequent 5G authentication procedures.

4 Performance Evaluation

This section evaluates the performance impact of the proposed SGX-based encrypted storage on the 5G authentication workflow. The evaluation focuses on three key metrics, namely CPU utilization, mem- ory consumption, and execution latency, during authentication data insertion and retrieval operations in the Unified Data Repository (UDR). These operations represent the most performance-critical com- ponents of the authentication process. Similar performance–security trade-offs have been reported in recent studies on roaming security, TLS optimization, and remote SIM provisioning in 5G and beyond networks [24, 25, 26].

All experiments were conducted on a virtualized testbed deployed on a commodity server equipped with an Intel Core i9-14900K CPU (24 cores, 32 threads) operating at a base frequency of 3.20 GHz, 64 GB DDR5 RAM, and an NVIDIA GeForce RTX 4070 GPU. The 5G core network was implemented using the OpenAirInterface platform, with the UDR backed by a MySQL database. Intel Software Guard Extensions (SGX) was enabled to host the encryption and decryption logic within a hardware-protected enclave. To evaluate end-to-end performance, more than 10,000 authentication attempts were executed, covering the complete workflow from User Equipment (UE) initialization to authentication completion. Three configurations were compared: Plain, where authentication data are stored without encryption; Encrypted without SGX, where encryption is applied outside a Trusted Execution Environment; and Encrypted with SGX, representing the proposed design.

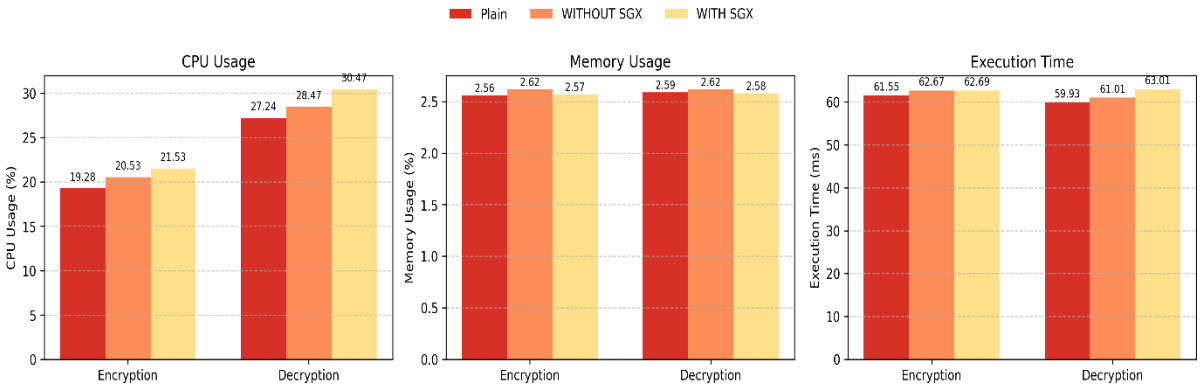

Figure 3: Performance comparison of authentication data operations in the UDR.

Figure 3 summarizes the performance impact of the proposed SGX-based encrypted storage across CPU utilization, memory consumption, and execution latency. CPU usage increases moderately with en- cryption, particularly during select operations. Insert operations show an increase from 19.28% (plain) to 20.53% without SGX and 21.53% with SGX, while select operations increase from 27.24% to 28.47% and 30.47%, respectively. This overhead is primarily attributed to enclave transitions and cryptographic processing inside the Trusted Execution Environment. In contrast, memory consumption remains largely unaffected, staying within a narrow range of 2.5–2.6% across all configurations, indicating negligible memory overhead even with SGX-enabled key isolation.

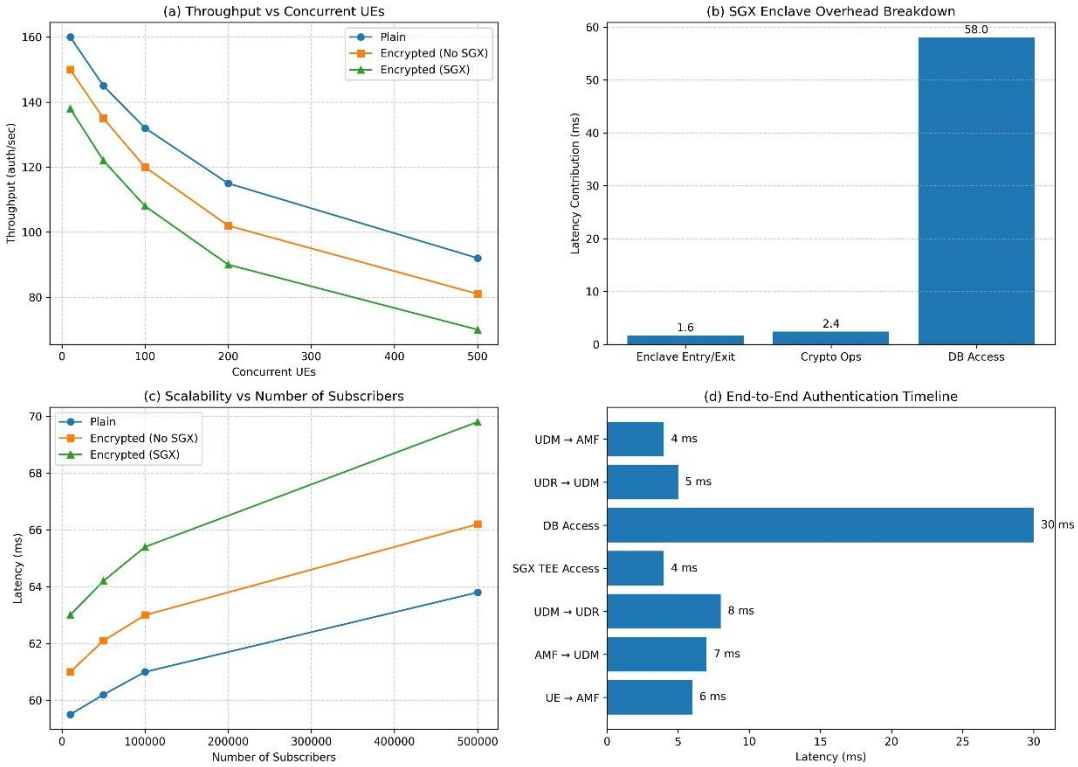

Figure 4: Comprehensive performance evaluation of the proposed SGX-based protected UDR.

Execution latency exhibits a similar trend. Insert operations incur average delays of 61.55 ms (plain), 62.67 ms (encrypted without SGX), and 62.69 ms (encrypted with SGX), while select operations in- crease from 59.93 ms to 61.01 ms and 63.01 ms, respectively. Although SGX introduces additional latency due to enclave entry and exit, the overall impact remains within a few milliseconds and does not significantly affect end to end authentication performance.

Figure 4 provides a broader performance perspective under realistic workload conditions. Fig- ure 4(a) shows that authentication throughput decreases gradually as the number of concurrent UEs increases, with the SGX-enabled configuration exhibiting lower throughput due to enclave overhead, yet maintaining stable operation at high concurrency levels. Figure 4(b) reveals that database access dominates overall latency, while enclave entry/exit and cryptographic operations contribute only minor overhead, confirming that SGX itself is not the primary bottleneck. Scalability results in Figure 4(c) indicate that authentication latency increases moderately with growing subscriber populations, with the SGX-based design incurring a bounded and predictable overhead. Finally, Figure 4(d) shows that end-to-end authentication latency is largely dominated by database access and inter-network-function communication, while SGX TEE access accounts for only a small fraction of the total delay.

Overall, these results demonstrate that the proposed SGX-based storage-centric protection achieves a favorable trade-off between security and performance. While CPU utilization increases during decryption-intensive operations, memory overhead is negligible and latency impact remains limited, confirming the practicality of Trusted Execution Environment-based data-at-rest protection for real- world 5G core deployments.

5 Conclusion and Future Work

This paper investigated the security risks of storing sensitive authentication data in the 5G core, with a particular focus on the Unified Data Repository (UDR) under server compromise scenarios. To address these risks, we proposed a storage-centric protection scheme that encrypts subscriber authentication data before database persistence and fully isolates cryptographic operations and key management inside an Intel Software Guard Extensions (SGX)-based Trusted Execution Environment (TEE). As a result, plaintext credentials and cryptographic keys are never exposed outside a hardware-protected enclave.

The proposed design was implemented in a real 5G core environment based on OpenAirInterface and evaluated through 10,000 end-to-end authentication attempts. Experimental results show that al- though SGX integration introduces moderate CPU overhead, especially during decryption-intensive retrieval operations, memory consumption remains negligible and latency overhead is limited to a few milliseconds. These findings confirm that strong data-at-rest protection for 5G authentication data can be achieved without prohibitive performance penalties, making the approach practical for real-world deployments. By hardening credential storage rather than focusing solely on protocol-level security, the proposed scheme significantly reduces the blast radius of database and application-layer compromises and provides effective mitigation against insider threats. This work complements existing 5G authentication mechanisms and enhances the overall resilience of the 5G core.

Future work will focus on optimizing enclave execution through techniques such as batching, reduced enclave transitions, and caching to further lower CPU overhead in large-scale deployments. In addition, extending the architecture to support alternative Trusted Execution Environments and confidential computing platforms would improve portability across heterogeneous hardware. Integrating post-quantum cryptographic primitives within the enclave is another promising direction to enhance long-term security. Finally, comprehensive security evaluations, including side-channel resistance, large-scale stress testing, and intelligent anomaly detection mechanisms, will be explored to further strengthen the robustness of the proposed solution [27, 28].

Acknowledgments

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government(MSIT) (No. RS-2024-00398312, Devel- opment of Quantum Security Based Device Identification and Test Verification Technologies for 5G Non-Public Network)

References

[1] TS 33.501: Security architecture and procedures for 5G system, 2018.

[2] Bonam Kim, Youngjoon Kim, InSung Lee, and Ilsun You. Design and implementation of a ubiquitous ecg monitoring system using sip and the zigbee network. In Proceedings of the Future Generation Communication and Networking Conference (FGCN 2007), pages 1–6, Jeju, South Korea, 2007. IEEE.

[3] Zack Whittaker. Timeline of sk telecom's data breach. TechCrunch, May 2025.

[4] C. L. Huth, D. W. Chadwick, W. R. Claycomb, and Ilsun You. Guest editorial: A brief overview of data leakage and insider threats. Information Systems Frontiers, 15(1):1–4, 2013.

[5] Abdullah Alshamrani et al. Threat modeling and mitigation of udr attacks in 5g core. Journal of Network and Computer Applications, 197:103270, 2022.

[6] Adi Panca Saputra Iskandar, Yongho Ko, Bonam Kim, Linawati, and Ilsun You. Formal and practical analysis of early-stage vulnerabilities in eap-tls 1.3 against ddos attacks. In Proceedings of the 2025 International Conference on Smart-Green Technology in Electrical and Information Systems (ICSGTEIS), pages 59–64, Denpasar, Bali, Indonesia, 2025. IEEE.

[7] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016:86, 2016.

[8] Wei Zheng, Jianfeng Hu, and Lei Zhang. Survey of intel sgx and its applications. Frontiers of Computer Science, 13(6):1242–1261, 2019.

[9] Jungwon Ahn and Sungjin Lee. Trusted execution environment-based secure storage systems. IEEE Access, 8:187312–187325, 2020.
[10] Bo Lai and Rui Zhang. Securing cloud databases using trusted execution environments. IEEE Transactions on Cloud Computing, 7(3):881–894, 2019.
[11] OpenAirInterface Software Alliance. Open-source 5g core network: Architecture and implementation. In IEEE ICC Workshops, 2020.
[12] Naveed Akhtar and Atta Rehman. A survey on security and privacy of 5g technologies. IEEE Communications Surveys & Tutorials, 23(1):368–408, 2021.
[13] Jaehyun Park and Youngho Kim. Security analysis of service-based architecture in 5g core networks. IEEE Access, 8:220353–220365, 2020.
[14] Jie Guan, Jian Cai, Hui Bai, and Ilsun You. Deep transfer learning-based network traffic classification for scarce dataset in 5g iot systems. International Journal of Machine Learning and Cybernetics, 12(11):3351–3365, 2021.
[15] Alexandros Dimitriadis and Panagiotis Papadimitriou. Security challenges and solutions in 5g core networks.Computer Networks, 192:108067, 2021.
[16] Markus Miettinen and Ahmad-Reza Sadeghi. Post-quantum cryptography in 5g and beyond. IEEE Security & Privacy, 18(3):38–46, 2020.
[17] Yongho Ko, I Wayan Adi Juliawan Pawana, and Ilsun You. 5G-AKA-HPQC: Hybrid post-quantum cryptography protocol for quantum-resilient 5g primary authentication with forward secrecy. arXiv preprint arXiv, 2025. Submitted on 5 February 2025.
[18] Taeho Won, Hoseok Kwon, Yongho Ko, Jhury Kevin Lastre, and Ilsun You. MoTH: Mobile terminal handover security protocol for hub switching based on 5g and beyond (5gb) p2mp backhaul environment. IEEE Internet of Things Journal, 9(16):14667–14684, 2022.
[19] Jiyoon Kim, Daniel Gerbi Duguma, Philip Virgil Astillo, Hoon-Yong Park, Bonam Kim, and Ilsun You. A formally verified security scheme for inter-gnb-du handover in 5g vehicle-to-everything. IEEE Access, 9:119100–119117, 2021.
[20] I Wayan Adi Juliawan Pawana, Vincent Abella, Jhury Kevin Lastre, Yongho Ko, and Ilsun You. Enhancing roaming security in cloud-native 5g core network through deep learning-based intrusion detection system. Computer Modeling in Engineering & Sciences, 145(2):2733–2760, 2025.
[21] Sergei Arnautov, Bohdan Trach, Franz Gregor, et al. Scbr: Shielded execution of unmodified applications. In USENIX Security Symposium, 2016.
[22] Intel Corporation. Intel software guard extensions programming reference. Intel Technical Documentation, 2023.
[23] Florian Tramer et al. Dark side of the enclave: Side-channel attacks on sgx. In USENIX Security Symposium, 2018.
[24] Taeho Won, Hoseok Kwon, Yongho Ko, Jhury Kevin Lastre, and Ilsun You. Towards 6g roaming security: Experimental analysis of suci-based dos, cost, and nf stress. Applied Sciences, 16(1):508, 2026.
[25] Jhury Kevin Lastre, Yongho Ko, Hoseok Kwon, and Ilsun You. Evaluating transport layer security 1.3 optimization strategies for 5g cross-border roaming: A comprehensive security and performance analysis. Sensors, 25(19):6144, 2025.
[26] Yongho Ko, Jhury Kevin Lastre, Hoseok Kwon, and Ilsun You. Revisiting the m2m remote sim provisioning protocol: A comprehensive security and performance analysis. Alexandria Engineering Journal, 135:1–19, 2026.
[27] I Wayan Adi Juliawan Pawana, Philip Virgil Astillo, and Ilsun You. Lightweight llm-based anomaly detection framework for securing iotmd enabled diabetes management control systems. IEEE Journal of Biomedical and Health Informatics, pages 1–12, 2025. Early Access.
[28] Hoonyong Park, Philip V. B. Astillo, Taeguen Kim, and Ilsun You. 5g native network function for false base station detection using machine learning technique. Wireless Networks, 2025. Published 5 June 2025.