# Extending Open5GS for IIoT: Performance Evaluation of the EAP-AKA' Integration for 5G Standalone Non-Public Networks

I Wayan Adi Juliawan Pawana[1,2], Hoseok Kwon[1], Vincent Abella[1], Bonam Kim[1], Ilsun You[1]

[1]Kookmin University, Seoul, South Korea

[2]Udayana University, Badung, Indonesia

Received: September 29, 2025; Revised: November 25, 2025; Accepted: December 23, 2025; Published: December 30, 2025

**Abstract**

The growing demands of the Industrial Internet of Things (IIoT) necessitate secure and flexible authentication in 5G Standalone Non-Public Network (SNPN). While the Extensible Authentication Protocol (EAP) supports such scenarios, open-source 5G cores, such as Open5GS, lack support for EAP-based methods and rely solely on 5G-AKA. This work adds EAP-AKA' support to Open5GS, enabling secure USIM-based authentication for SNPN. A virtualized testbed was used to compare EAP-AKA' with standard 5G-AKA. Results show that EAP-AKA' increases message size, latency, and memory usage due to EAP encapsulation and ECIES-based cryptographic operations. Despite the added overhead, EAP-AKA' improves authentication flexibility. This enhancement makes Open5GS more suitable for private 5G deployments in industrial environments, aligning it with 3GPP standards for secure and scalable authentication.

**Keywords:** IIoT, EAP-AKA', SNPN, Private 5G.

## 1 Introduction

The Industrial Internet of Things (IIoT) is fundamentally reshaping the manufacturing and logistics landscape by enabling seamless interconnection and data sharing among machines, sensors, and control systems. This digital transformation relies heavily on communication networks capable of delivering Ultra-Reliable Low-Latency Communication (URLLC), massive device density, and high throughput [1,2,3,4]. Fifth-generation (5G) mobile networks have emerged as the primary enabler for these requirements. They offer a scalable and secure foundation for smart buildings, smart agriculture, and healthcare applications [5,6,7,8].

However, the proliferation of IIoT devices introduces a significant expansion of the attack surface. Industrial environments are increasingly vulnerable to various cyber-attacks, ranging from data leakage and insider threats to sophisticated denial-of-service (DoS) attacks [9]. Furthermore, the inherent diversity of IIoT traffic is often characterized by scarce labeled data and limited computing resources. This makes traditional intrusion detection systems (IDS) difficult to deploy. Recent advances suggest that deep learning and large language model can mitigate these challenges in 5G IoT systems by enabling efficient traffic classification even with minimal datasets [10,11,12].

To meet the stringent security and operational demands of industrial enterprises, 3GPP introduced SNPN, which provide localized control and seamless integration with non-3GPP access. However, these environments face critical infrastructure-level threats, most notably from False Base Stations (FBS) attempting to intercept signaling or disrupt services [13,14]. Furthermore, the mobility of IIoT devices introduces significant vulnerabilities during the 5G handover process, where securing inter-node transitions is vital to prevent session

*DOI: https://doi.org/10.64799/rebicte.v11i.224*

hijacking and unauthorized context access [15]. Consequently, the primary authentication mechanism in an SNPN must serve as a resilient that protects the device lifecycle across both initial network access and subsequent mobility event.

The EAP framework is central to this flexibility. While 5G-AKA is the standard for 3GPP access, EAP-based methods like EAP-AKA' [16] are essential for non-3GPP integration and enhanced subscriber privacy. Current research explores future-proof concepts like Hybrid Post-Quantum Cryptography (HPQC) for quantum-resilient 5G authentication [17,18]. However, there is still a practical gap in the availability of these tools in open-source ecosystems

Specifically, Open5GS, which is a prominent open-source 5G core implementation, currently lacks native support for EAP-AKA'. This limitation hinders its utility in professional SNPN deployments that require standards-compliant, USIM-based authentication over non-3GPP access. This paper addresses this gap by detailing the implementation of EAP-AKA' within the Open5GS framework. We provide a comparative analysis between EAP-AKA' and 5G-AKA, evaluating their performance and security benefits within an IIoT context. Our contribution enhances the flexibility of open-source 5G cores and supports the deployment of secure, scalable, and resilient private networks.

## 2 Background

This section provides foundational context on 5G core network architecture, intrusion detection approaches, and deep learning architectures relevant to this study.

### 2.1 Standalone Non-Public Networks (SNPN)

A SNPN represents a significant advancement in industrial connectivity, allowing enterprises to deploy a complete 5G system independently of public mobile network operators [19,20,21,22,23]. Unlike Public Network Integrated NPNs (PNI-NPN), which share infrastructure or functions with a Public Land Mobile Network (PLMN), an SNPN is a self-contained environment that does not rely on the network functions of a public provider. This independence is vital for smart factories, warehouses, and remote campuses where data sovereignty and operational resilience are paramount.

Identification and Network Selection

In accordance with 3GPP Release 16, each SNPN is uniquely identified by the combination of a PLMN ID and a Network Identifier (NID). This dual identification system allows a User Equipment (UE) to discover and select a specific private network even when multiple SNPNs share the same PLMN ID. Within industrial environments, this mechanism prevents unauthorized devices from attempting to attach to sensitive local infrastructure. The identification process is closely linked to the security posture of the network, as the UE must be specifically provisioned with the correct NID to gain access.

Credential Management and the Credentials Holder (CH)

A critical feature introduced in 3GPP Release 17 is the concept of a Credentials Holder (CH) [16]. An SNPN can authenticate a UE using credentials managed by a separate entity, such as another SNPN, a public PLMN, or an external AAA server. This flexibility is essential for large scale IIoT deployments where devices may be manufactured with third-party credentials. Furthermore, Release 17 introduced formal procedures for UE onboarding and remote provisioning. This allows a UE to connect to a specialized Onboarding Network (ONN) to securely obtain the necessary SNPN credentials over the air. Such mechanisms are vital for managing the complex Machine-to-Machine (M2M) provisioning lifecycle required in dense sensor environments [24].

Security Integration and Industrial Reliability

Security in an SNPN is built upon the foundational EAP framework, which 3GPP integrated into the 5G core to support a wide range of authentication protocols. By utilizing the EAP framework, SNPNs can implement robust methods such as EAP-AKA' [25] and EAP-TLS [26,27]. These methods provide mutual authentication and secure key derivation.

## 2.2 EAP Framework in SNPN

The EAP framework [28] serves as a vital enabler for secure and adaptable authentication within SNPNs. Unlike previous generations where EAP was primarily utilized for non-3GPP access, the 5G architecture integrates EAP as a core component to support a broad range of credentials and access technologies. This flexibility is critical for industrial and enterprise environments characterized by diverse security and operational requirements. By allowing the network to authenticate users and devices using both 3GPP and non-3GPP identities, the EAP framework ensures that SNPNs can maintain a high bar for security while remaining scalable.

In the context of 5G security architecture, the EAP framework allows the Authentication Server Function (AUSF) to act as a backend EAP server, while the Security Anchor Function (SEAF) within the Access and Mobility Management Function (AMF) serves as a pass-through authenticator. This decoupling ensures that the AMF does not need to support every specific authentication method, as it simply facilitates the exchange of EAP messages between the UE and the AUSF. The primary functional scenarios for EAP within an SNPN are detailed below.

First, EAP enables secure Non-3GPP Access Authentication. This allows industrial devices to connect via access technologies such as Wi-Fi or Ethernet while using 3GPP credentials. By utilizing EAP-AKA', the network maintains a consistent authentication framework regardless of the access type, ensuring that the same level of cryptographic protection is applied across the entire industrial site. This is particularly useful for mobile robotic units that may switch between 5G NR and private Wi-Fi networks without requiring separate credential sets.

Second, the framework provides Alternative Authentication for IoT Devices. IIoT sensors that lack the hardware to support 3GPP AKA procedures can utilize methods such as EAP-TLS for certificate-based authentication or EAP-TTLS for legacy credentials. These methods are essential for offline or autonomous deployments where a central subscriber database may not be continuously reachable. The mandate for EAP-TLS 1.3 in SNPNs ensures strong mutual trust and provides forward secrecy, which is vital for protecting the integrity of critical control systems.

Third, the framework supports Flexible Identity and Method Support through the use of the Network Access Identifier (NAI) format. By utilizing the *username@realm* structure, the SNPN can implement domain-based routing and apply specific EAP methods to enforce custom security policies. For instance, an SNPN can distinguish between internal employees and guest hardware, applying EAP-AKA' to the former and EAP-TLS to the latter to maintain strict access control.

Finally, EAP facilitates Third-Party Credential Authentication. An SNPN can delegate the authentication process to external credential holders (CH), such as AAA servers, by utilizing the Network Slice Specific Authentication and Authorization Function (NSSAAF). Based on the identity domain of the user, the network routes EAP messages to the appropriate provider, which enables federated access control. This capability allows industrial partners to collaborate within a shared private 5G infrastructure while maintaining independent control over their own security credentials.

The security context established through these EAP methods is robust. For EAP-AKA', 3GPP Release 17 specifies that the 5G-specific key $K_{AUSF}$ is derived from the Extended Master Session Key (*EMSK*). This ensures that the master key material remains securely within the AUSF and does not leave the home network environment. Furthermore, the key hierarchy is bound to the serving network name, which prevents bidding-down attacks and ensures that the authentication is cryptographically tied to the specific access point being used.

### 2.3 EAP-AKA’

EAP-AKA’ is an enhanced authentication method designed for 5G systems as specified in RFC 9048 [25]. It extends the standard EAP-AKA by utilizing modified key derivation techniques, specifically the use of $CK'$ and $IK'$ instead of the original $CK$ and $IK$. This design mitigates known vulnerabilities and ensures cryptographic separation across different access networks. In this framework, the UE acts as the EAP peer, the SEAF serves as a pass-through authenticator, and the AUSF operates as the backend authentication server.

The procedure begins with initiation when the SEAF establishes a signalling connection with the UE. The UE provides its identity using a SUCI or a 5G Globally Unique Temporary Identifier (5G-GUTI). The AUSF receives this request, validates the authorization of the serving network name, and communicates with the Unified Data Management (UDM). If a SUCI is present, the Subscription Identifier De-concealing Function (SIDF) retrieves the permanent identifier (SUPI) using the private key of the home network.

During the challenge phase, the UDM generates an Authentication Vector (*AV*) comprising the *RAND*, *AUTN* , *XRES*, $CK'$, and $IK'$. The AUSF then sends an EAP-Request/AKA′-Challenge to the UE, which includes the *AT_KDF* attribute to specify the key derivation function. The UE verifies the *AUTN* and checks the separation bit in the Authentication Management Field to ensure protocol consistency. After successful verification, the UE computes the response (*RES*) and derives the local $CK'$ and $IK'$ to generate a Master Key (*MK*) and an integrity key $K_{aut}$.

The final verification occurs at the AUSF, where the received *RES* is compared against the expected *XRES* from the UDM. Upon a match, the AUSF derives the 256-bit anchor key $K_{AUSF}$ from the *EMSK*. This $K_{AUSF}$ serves as the basis for deriving $K_{SEAF}$ , which is then transmitted to the SEAF along with an EAP Success message. This hierarchical key derivation ensures that the 5G security context is securely anchored in the serving network while protecting long-term credentials. The complete authentication sequence is illustrated in Figure. 1.

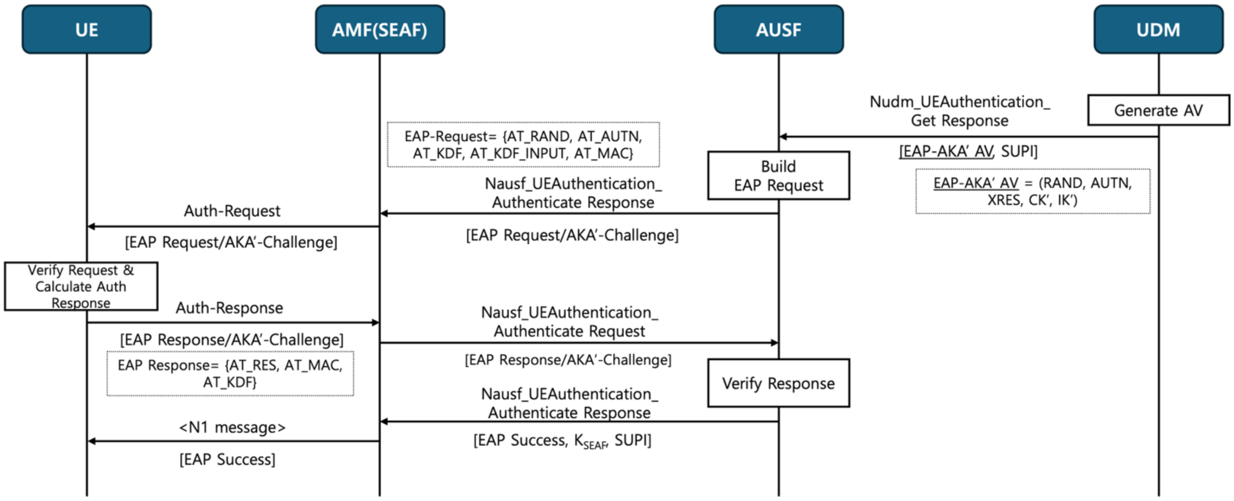

Figure 1. EAP-AKA’ Authentication Procedure.

# 3 Implementation Details

The evaluation of the EAP-AKA' and 5G-AKA frameworks was conducted within a virtualized cloud-native environment. The architectural setup for this experiment are illustrated in Figure. 2. This section details the experimental testbed, the software configurations, and the parameters used for the comparative analysis.

## 3.1 Experimental Testbed and Hardware

The environment was orchestrated using VMware Workstation 17, utilizing two distinct Virtual Machines (VMs) to isolate the core network functions from the access network components. Both VMs operated on Ubuntu 24.04.2 LTS

- **5G Core Node**: This VM hosted the Open5GS (v2.7.5) core network. To simulate a production-grade containerized environment, the core was deployed within a MicroK8s (v1.32.3) Kubernetes cluster. The node was provisioned with a 6-core CPU, 16 GB of RAM, and 100 GB of NVMe storage to ensure sufficient overhead for cryptographic processing and log analysis.
- **UE and RAN Node**: The second VM functioned as a combined UE and Radio Access Network (RAN) emulator using UERANSIM (v3.2.7). It was configured with a 4-core CPU and 4 GB of RAM, representing the typical resource constraints of an edge-computing gateway or a high-end IIoT controller.

## 3.2 Simulation Scenario and Configuration

To assess the performance of the authentication procedures under realistic load conditions, we implemented a sequential registration scenario. A total of 100 UEs were configured to register with the SNPN. A 1000 ms inter-arrival delay was introduced between each registration attempt to allow for the precise measurement of individual authentication latencies.

The experiments were conducted across three distinct Subscription Concealed Identifier (SUCI) protection schemes to evaluate the computational trade-offs:

1. **Null Scheme**: No encryption applied to the SUPI.
2. **Profile A**: Utilizing Elliptic Curve Integrated Encryption Scheme (ECIES) based on the Curve25519 algorithm.
3. **Profile B**: Utilizing ECIES based on the secp256r1 curve.

By varying these schemes across both 5G-AKA and EAP-AKA', we established a comprehensive baseline to measure the impact of EAP encapsulation and cryptographic overhead on the overall network performance.

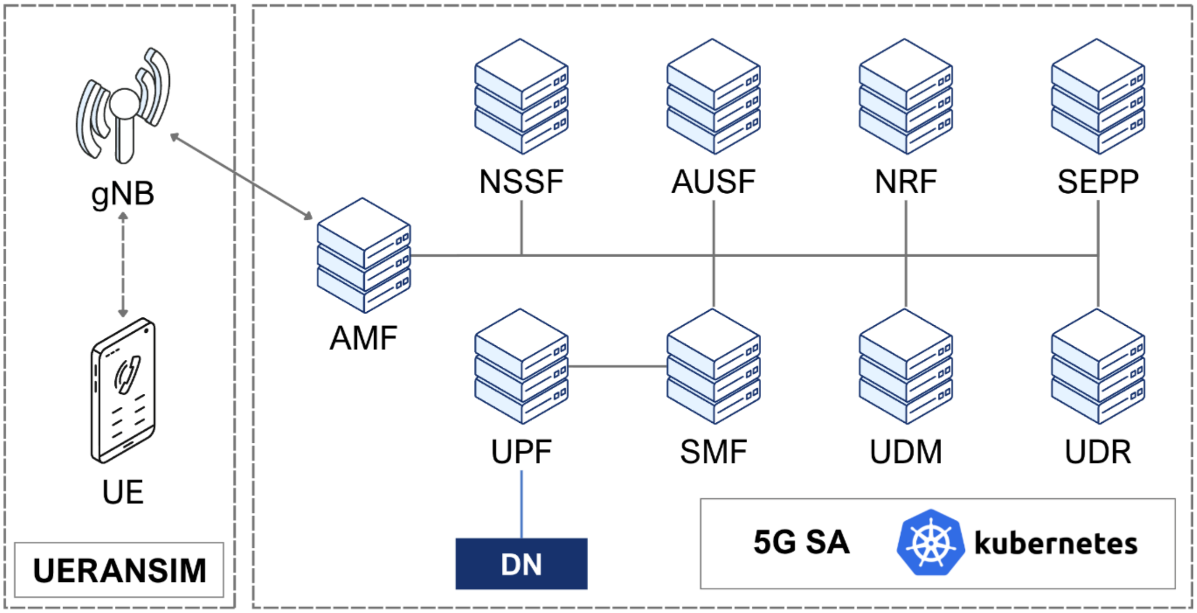

Figure 2. Experimental Testbed Architecture.

# 4 Experimental Results and Analysis

This section presents a quantitative evaluation of the implemented EAP-AKA’ protocol within the Open5GS framework, focusing on signaling overhead, authentication latency, and resource utilization. The performance is benchmarked against the standard 5G-AKA procedure across different SUCI protection profiles.

## 4.1 Signaling and Message Size Overhead

The impact of EAP encapsulation on the signaling plane is summarized in Table 1. The results indicate that EAP-AKA’ introduces a significant increase in message sizes across the majority of the authentication steps. While the initial response from the UDM to the AUSF remains consistent at 80 bytes for both methods, the subsequent challenge and response phases exhibit a notable overhead. The Nausf_UEAuthentication Authenticate Response from the AUSF to the AMF increases from 48 bytes in 5G-AKA to 108 bytes in EAP-AKA’, representing a 125 percent increase. This expansion is primarily attributed to the inclusion of specialized EAP attributes such as ATRAND, ATAUTN, AT KDF , and AT M AC. Similarly, the Authentication Request sent from the AMF to the UE grows from 32 bytes to 108 bytes. The UE response size also increases by 175 percent, rising from 16 bytes to 44 bytes to accommodate the EAP payload. These findings suggest that while EAP-AKA’ provides superior flexibility for non-3GPP access in industrial environments, it requires higher signaling bandwidth compared to the more optimized 5G-AKA.

Table 1. Message Sizes Overhead

| NF | Message | 5G-AKA | EAP-AKA’ |
|---|---|---|---|
| UDM → AUSF | Nudm_UEAuthentication_Get Response | 80 | 80 |
| AUSF → AMF | Nausf_UEAuthentication_Authenticate Response | 48 | 108 |
| AMF → UE | Auth-Request | 32 | 108 |
| UE → AMF | Auth-Response | 16 | 44 |
| AMF → AUSF | Nausf_UEAuthentication_Authenticate Request | 16 | 44 |
| AUSF → AMF | Nausf_UEAuthentication_Authenticate Response | 32 | 36 |

### 4.2 Authentication Latency Analysis

Authentication latency is a critical metric for IIoT applications, particularly for mobile units requiring rapid network re-entry. Table 2 provides a comprehensive breakdown of latency measurements. The data reveals that the 5G-AKA Null Scheme achieves the lowest average latency at 0.0194 seconds. In contrast, EAP-AKA' using Profile A (ECIES-based protection) exhibits the highest average latency at 0.0585 seconds, with a maximum peak of 0.462 seconds.

The increased latency in EAP-AKA' is a result of the combined overhead of EAP packet encapsulation and the cryptographic complexity of the chosen protection profile. Profile A and Profile B both demonstrate higher processing times than the Null Scheme due to the intensive computations required for ECIES deconcealment. Notably, EAP-AKA' Profile A shows a higher standard deviation (0.0731s) compared to its 5G-AKA counterpart (0.0439s). This suggests that the EAP state machine and attribute parsing within the AUSF and UE introduce additional jitter into theauthentication process.For mission-critical IIoTscenaros, these latency trade-offs must be balanced against the security requirements of the specific industrial application.

Table 2. Authentication Latency

| Auth Method | Avg(s) | Min(s) | Max(s) | Std(s) | P50(s) | P90(s) | P95(s) | P99(s) |
|---|---|---|---|---|---|---|---|---|
| 5G-AKA Null Scheme | 0.0194 | 0.013 | 0.266 | 0.0421 | 0.028 | 0.05 | 0.0592 | 0.26302 |
| 5G-AKA Profile A | 0.0438 | 0.016 | 0.261 | 0.0439 | 0.0325 | 0.0571 | 0.08 | 0.25307 |
| 5G-AKA Profile B | 0.0398 | 0.014 | 0.263 | 0.0407 | 0.03 | 0.056 | 0.0638 | 0.26108 |
| EAP-AKA' Null Scheme | 0.0246 | 0.012 | 0.226 | 0.0389 | 0.017 | 0.02 | 0.2222 | 0.22208 |
| EAP-AKA' Profile A | 0.0585 | 0.017 | 0.462 | 0.0731 | 0.032 | 0.2115 | 0.2492 | 0.27495 |
| EAP-AKA' Profile B | 0.0575 | 0.016 | 0.410 | 0.0689 | 0.036 | 0.0856 | 0.2462 | 0.3108 |

### 4.3 Memory Utilization and Resource Impact

The impact of the authentication procedures on system resources is illustrated in Figure 3. Both 5G-AKA and EAP-AKA' contribute to increased memory utilization across the network functions (NFs), particularly the AUSF and UDM. This trend is most pronounced when using Profile A and Profile B.

The rise in memory consumption is directly linked to the cryptographic operations inherent in the Elliptic Curve Integrated Encryption Scheme (ECIES). The implementation requires temporary memory allocation for coordinate calculations, key derivation functions (KDF ), and MAC verification buffers. Although EAP-AKA' introduces additional protocol logic, the primary driver for memory spikes remains the SUCI de-concealment process rather than the EAP framework itself. These results indicate that while the Open5GS implementation of EAP-AKA' is functionally robust, resource-constrained IIoT gateway devices must be provisioned with sufficient memory to handle the cryptographic load of certificate-based or ECIES-protected identities.

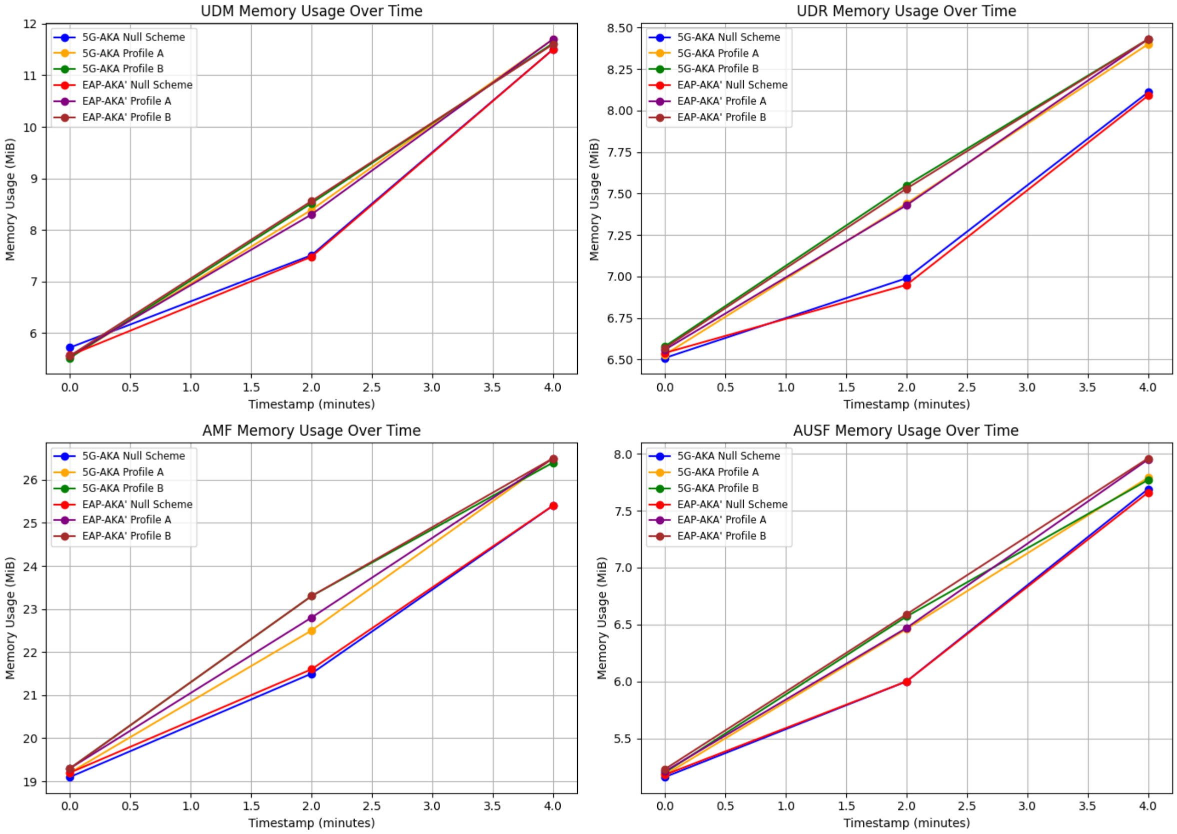

Figure 3. Memory Utilization across Network Function.

# 5 Conclusion

This paper presented the successful implementation and evaluation of the EAP-AKA' authentication protocol within the Open5GS framework, addressing a critical gap in open-source 5G core support for SNPN. By integrating EAP- AKA' into the AUSF and UDM modules, this work enables standards-compliant, USIM-based authentication over both 3GPP and non-3GPP access technologies. Such enhancements are vital for the deployment of secure and flexible private 5G networks in industrial environments.

The experimental results highlighted the inherent trade-offs between security and performance. The analysis confirmed that EAP-AKA' introduces a significant signaling overhead, with message sizes increasing by up to 125 percent due to EAP encapsulation and the inclusion of specialized attributes. Furthermore, authentication latency was noticeably higher when paired with ECIES-based SUCI protection profiles. While these factors increase processing time and memory consumption, they provide the cryptographic binding and access network independence required for high-security IIoT deployments.

Moving forward, we intend to further enhance SNPN flexibility by implementing EAP-TLS and EAP-TTLS support within the Open5GS core. This extension will facilitate seamless authentication for IoT devices that lack USIM hardware by enabling the use of digital certificates or legacy credentials. By expanding the range of supported EAP methods, we aim to provide a more inclusive security framework for heterogeneous IIoT ecosystems. This ongoing work provides a robust foundation for researchers and private network operators to explore secure, localized 5G connectivity without relying on proprietary core implementations.

Acknowledgement

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT).

Funding Details

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

## References

[1] Aamir Mahmood, Luca Beltramelli, Sarder Fakhrul Abedin, Shah Zeb, Nishat I. Mowla, Syed Ali Hassan, Emiliano Sisinni, and Mikael Gidlund. Industrial IoT in 5G-and-Beyond Networks: Vision, Architecture, and Design Trends. IEEE Transactions on Industrial Informatics, 18(6):4122–4137, 2022.

[2] Jiyoon Kim, Philip Virgil Astillo, Vishal Sharma, Nadra Guizani, 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.

[3] Xiaohu Yo et all. Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Science China Information Sciences, 64(1):110301, 2020.

[4] Fengxian Guo, F. Richard Yu, Heli Zhang, Xi Li, Hong Ji, and Victor C. M. Leung. Enabling Massive IoT Toward 6G: A Comprehensive Survey. IEEE Internet of Things Journal, 8(15):11891–11915, 2021

[5] Agbotiname Lucky Imoize, Oluwadara Adedeji, Nistha Tandiya, and Sachin Shetty. 6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap. Sensors, 21(5), 2021.

[6] Xing Yang, Lei Shu, Jianing Chen, Mohamed Amine Ferrag, Jun Wu, Edmond Nurellari, and Kai Huang. A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges. IEEE/CAA Journal of Automatica Sinica, 8(2):273–302, 2021.

[7] Pal Varga, Jozsef Peto, Attila Franko, David Balla, David Haja, Ferenc Janky, Gabor Soos, Daniel Ficzere, Markosz Maliosz, and Laszlo Toka. 5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps. Sensors, 20(3), 2020

[8] 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 Future Generation Communication and Networking (FGCN 2007), volume 2, pages 599–604, 2007.

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

[10] Jianfeng Guan, Junxian Cai, Haozhe 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.

[11] I Wayan Adi Juliawan Pawana, Vincent Abella, Jhury 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.

[12] 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.

[13] Hoonyong Park, Philip V. B. Astillo, Taeguen Kim, and Ilsun You. 5G Native Network Function for False Base Station Detection Using Machine Learning Technique. Information Systems Frontiers, 2025.

[14] Yeongshin Park, I Wayan Adi Juliawan Pawana, Bonam Kim, and Ilsun You. Harnessing GAN to Create Realistic FBS(False Base Station) Attack Data in 5G. In 2024 IEEE International Symposium on Consumer Technology (ISCT), pages 404–408.

[15] Jiyoon Kim, Daniel Gerbi Duguma, Philip Virgil Astillo, Hoon-Yong Park, Bonam Kim, Ilsun You, and Vishal Sharma. A Formally Verified Security Scheme for Inter gNB-DU Handover in 5G Vehicle-to-Everything. IEEE Access, 9:119100–119117,2021.

[16] 3rd Generation Partnership Project (3GPP). System Architecture for the 5G System (5GS); Stage 2. Technical Report TS 23.501, 3GPP, March 2024. [Online]. Available:

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

[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, 2025.

[18] Hoseok Kwon, Yongho Ko, I Wayan Adi Juliawan Pawana, and Ilsun You. Toward Quantum-Safe 6G Mobile Networks: A Survey on EAP-AKA Prime Family with Formal Security Analysis and Empirical Evaluation. IEEE Transactions on Consumer Electronics, 2025.

[19] Adnan Aijaz. Private 5G: The Future of Industrial Wireless. IEEE Industrial Electronics Magazine, 14(4):136–145, 2020.

[20] Miaowen Wen, Qiang Li, Kyeong Jin Kim, David López-Pérez, Octavia A. Dobre, H. Vincent Poor, Petar Popovski, and Theodoros A. Tsiftsis. Private 5G Networks: Concepts, Architectures, and Research Landscape. IEEE Journal of Selected Topics in Signal Processing, 16(1):7–25, 2022.

[21] Jonathan Prados-Garzon, Pablo Ameigeiras, Jose Ordonez-Lucena, Pablo Muñoz, Oscar Adamuz-Hinojosa, and Daniel Camps-Mur. 5G Non-Public Networks: Standardization, Architectures and Challenges. IEEE Access, 9:153893–153908, 2021.

[22] 3rd Generation Partnership Project (3GPP). Service requirements for the 5G system; Stage 1. Technical Report TS 22.261, 3GPP, December 2024. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107.

[23] 3rd Generation Partnership Project (3GPP). Non-Public Networks (NPN). 3GPP Technology Page, 2024. [Online]. Available: https://www.3gpp.org/technologies/npn. Accessed: Jan. 2026.

[24] 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

[25] Jari Arkko, Vesa Lehtovirta, Vesa Torvinen, and Pasi Eronen. Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA'). RFC 9048, October 2021.

[26] Bernard Aboba, Dirk Simon, and Paul R. Simon. The EAP-TLS Authentication Protocol. RFC 5216, March 2008.

[27] Jingjing Zhang, Lin Yang, Weipeng Cao, and Qiang Wang. Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif. IEEE Access, 8:23674–23688, 2020.

[28] Bernard Aboba, Mark Blunk, John Vollbrecht, James Carlson, and Henrik Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748, June 2004.