# Design Framework for Intelligent Security Event Integration in 5G Private Networks

*Taeuk Park
ICT Device Research Center
GERI(Gumi Electronics & Information Technology Research Institute)
Gumi, Korea
Department of IT Convergence Engineering, Kumoh National Institute of Technology
Gumi, Korea
ptu@geri.re.kr

Mahnsuk Yoon
ICT Device Research Center
GERI(Gumi Electronics & Information Technology Research Institute)
Gumi, Korea
yms@geri.re.kr

Jaeuk Kwon
ICT Device Research Center
GERI(Gumi Electronics & Information Technology Research Institute)
Gumi, Korea
kwonjuk@geri.re.kr

***Abstract*—With the increasing adoption of 5G private networks across industrial domains such as smart factories, intelligent logistics, and remote healthcare, network architectures are evolving into complex systems that integrate with enterprise networks. However, conventional security frameworks fall short of meeting the requirements of these environments, which demand real-time threat detection, interoperability among heterogeneous systems, and operator-oriented visibility [1].**

**In this study, we propose an integrated security architecture for intelligent event detection and response in 5G private networks. The architecture encompasses five modularized functions: real-time traffic collection, data preprocessing, anomaly detection, policy-based response, and interactive visualization. Key components include GTP-U–based traffic collection, flow-statistics vector generation, rule- and policy-driven detection and response logic, and RESTful API–based interoperability.**

**Given that the study is in an early design phase without experimental implementation, we evaluate the feasibility of the proposed system through practical deployment scenarios, including abnormal device behavior detection and inter-system event correlation [3]. Evaluation criteria are defined based on detection sensitivity, time-to-detect (TTD), system interoperability, and operator visibility. This framework is expected to serve as a foundational design for future implementations, including AI-based detection integration, SOAR (Security Orchestration, Automation, and Response) systems, and testbed-based validation.**

***Keywords —5G Private Network, Security Architecture, Real-time Threat Detection, GTP-U Traffic Monitoring, Security Data Preprocessing, Anomaly Detection, Policy-based Response, Security Visualization, Heterogeneous Network Integration, Modular Security Framework***

## I. INTRODUCTION

5G mobile communication has been rapidly adopted across various industrial domains, driven by its core features: ultra-high-speed data transmission, ultra-low latency, and massive device connectivity. In particular, the so-called "5G private networks" are private networks independently deployed to meet the requirements of specific industries, and are emerging as a key infrastructure for applications such as smart factories, intelligent logistics, and remote healthcare. These networks offer tailored quality-of-service (QoS) capabilities; however, their architecture and operational models differ significantly from those of conventional public networks. As a result, they often involve heterogeneous system integrations and expose new vectors of cybersecurity threats [1][2].

Traditional security systems have primarily relied on fixed, policy-based access controls and post-event intrusion detection mechanisms. Such approaches, however, are insufficient in environments where real-time detection, cross-system interoperability, and operator-centric visibility are simultaneously required—typical of the integrated 5G enterprise and control network landscapes [3]. As 5G private networks increasingly interconnect with enterprise networks, operational systems, and service domains, the need for a unified, real-time threat detection and response framework becomes critical.

This study aims to design an integrated security system architecture that addresses the unique technical requirements of the 5G private network environment. The proposed architecture encompasses five core functions: real-time data collection, preprocessing, anomaly detection, policy-based response, and operator-facing visualization. Given the pre-implementation stage of this research, emphasis is placed on validating the structural feasibility of the architecture through module design and data flow specification. Key design features include a real-time traffic collection model optimized for flow analysis, a GTP-U-based anomaly detection policy, a policy-driven response logic, a GUI-oriented monitoring framework, and a standardized interface for interoperable security system integration.

The structural contributions of this study are as follows:
(1) We derive a set of architectural requirements for real-time integrated security in 5G private–enterprise hybrid environments.
(2) We propose a modularized system structure that supports real-time traffic collection, preprocessing, detection, visualization, and external system integration.
(3) We develop a feasible security architecture based on GTP-U traffic analysis and policy-coordinated response workflows.
(4) We present an application scenario and structure-based evaluation framework that verifies the technical feasibility and practical applicability of the design, even in the absence of system implementation.

## II. Related Work

Research on security frameworks for 5G networks has been actively conducted across various domains, including user-plane traffic analysis, AI-based anomaly detection, and real-time threat monitoring architectures. This section classifies related work into three categories and discusses their structural distinctions and limitations, highlighting the contribution of this study.

**First**, several studies have focused on anomaly detection based on the GTP-U protocol, which is responsible for transporting user-plane data in 5G networks. In the legacy 4G/EPC environment, techniques such as Markov models and machine learning were employed to detect fuzzing attacks using GTP-C control messages; these approaches, however, were primarily post-analysis in nature. In contrast, recent 5G-oriented methods leverage the real-time characteristics of high-speed traffic by applying deep learning-based techniques that collect and analyze GTP-U packets on the fly. These advances align with this study's architectural direction, which involves real-time event processing and anomaly detection over GTP-U traffic [14].

**Second**, several efforts have been made to build realistic 5G security datasets and apply AI-based detection techniques. Samarakoon et al. [1] collected traffic data from a 5G testbed to train machine learning models for intrusion detection. Radoglou-Grammatikis et al. [2] constructed a statistical dataset based on PFCP flows and publicly released it, laying the foundation for anomaly detection systems applicable to 5G cores. These prior efforts provide empirical support for the necessity and feasibility of real-time data collection and preprocessing, as pursued in this research.

**Third**, recent studies have proposed real-time security frameworks that combine explainable AI (XAI) and integrated operator interfaces. For example, the 5GCIDS framework proposed by Radoglou-Grammatikis et al. [3] integrates convolutional neural networks (CNNs) with SHAP-based interpretability to improve both administrator awareness and detection reliability. However, many of these studies emphasize specific functional components—such as detection engines or visualization tools—rather than proposing full-stack architectural solutions that cover data ingestion, preprocessing, detection, policy-based response, and inter-system interoperability [14].

To summarize, existing research has mainly concentrated on enhancing detection accuracy, building labeled datasets, or improving interpretability for operators. In contrast, this study adopts a holistic architectural perspective that includes GTP-U–based flow statistics modeling, modular anomaly detection and response logic, and standardized interfaces for cross-domain system integration. Table I provides a comparative summary of representative prior works and the proposed approach.

TABLE I. Comparison of Related Works and the Proposed Approach

| Study | Real-Time. | GTP | Prep. | Detect. | Policy | GUI | Het. Sys. |
|---|---|---|---|---|---|---|---|
| Research A | X | X | √ | ML | X | X | X |
| Research B | √ | X | √ | DL | √ | X | X |
| This Work | √ | √ | √ | R/B | √ | √ | √ |

**Note**: *Prep.* = Preprocessing; *Detect.* = Detection Method; *GUI* = Graphical Monitoring Interface; *Het. Sys.* = Heterogeneous System Integration; *ML* = Machine Learning; *DL* = Deep Learning; *R/B* = Rule-Based.

## III. System Requirements and Design Principles

### A. Characteristics and Challenges of 5G private Network Security Integration

The 5G private network is designed to support ultra-high-speed, low-latency, and high-capacity communications, and is fundamentally structured to interact with enterprise private networks and industrial systems. In such environments, real-time data exchange across heterogeneous systems and complex security interoperation are essential, giving rise to distinct technical security challenges not encountered in traditional commercial networks [4][5].

First, there is a growing need for real-time traffic analysis. The average variation cycle of user plane traffic in 5G networks is extremely short—often within a few seconds—necessitating the detection of anomalous behavior with minimal delay. In this context, the detection delay, or Time-To-Detect (TTD), must be minimized and is defined by the following equation:

$$TTD = T_{alert} - T_{event}$$

Eq. 1. Time-To-Detect (TTD) Calculation

Here, $T_{event}$ denotes the timestamp of the anomalous event occurrence, and $T_{alert}$ is the timestamp at which the alert is generated. For effective real-time response, TTD should ideally be maintained under one minute [2].

Second, interoperability between heterogeneous security systems is required. Integration between different security devices such as firewalls, intrusion detection systems (IDS), and policy servers is critical to enable effective event correlation and policy enforcement. A failure in interoperation may lead to missed detections and delayed responses [6].

Third, ensuring operator visibility remains a crucial challenge. The system must provide interfaces that allow for intuitive tracking and visualization of threat flows at the device or session level, supporting situational awareness for human operators [3].

Finally, the centralized integration and normalization of multi-source events are essential. The platform should unify diverse events into a standardized format and support priority-based classification and policy-driven response.

Given these challenges, a single-purpose detection system is insufficient. A security architecture that simultaneously satisfies the requirements of real-time responsiveness, inter-system interoperability, automation, and visibility is indispensable.

### B. Definition of Integrated Security Requirements

Based on the above analysis, this study derives a set of core technical requirements for an integrated security system operating in a 5G SN and enterprise network hybrid environment.

From the data acquisition perspective, the system must capture GTP-U based user plane traffic in real time and

extract detailed statistics at the terminal and session levels. The collection interval should be under 60 seconds and should support asynchronous detection of high-frequency events [1].

In terms of preprocessing and integration, raw traffic data must be transformed into a flow vector format suitable for use by detection algorithms. The system must perform outlier removal, normalization, and session-level flow structuring. The flow vector structure used in this study is defined as:

$$F_i = [n_{pkt,}\, b_{total,}\, d_{sess,}\, p_{src,}\, p_{dst,}\, t_{start,}\, t_{end,}\, f_{proto,}\, f_{label}]$$

Eq. 2. Definition of Flow Vector $F_i$ for Real-Time Anomaly Detection

Each flow vector $F_i$ consists of nine components: total packet count ($n_{pkt}$), byte volume ($b_{total}$), session duration ($d_{sess}$), source and destination ports ($p_{src,}$ $p_{dst}$), start and end times ($t_{start,}$ $t_{end}$), protocol type ($f_{proto}$), and a label for classification of AI training ($f_{label}$). These features enable effective detection of abnormal traffic spikes, unauthorized port usage, and anomalous session behaviors [14]. Furthermore, the vector format is flexible enough to support both rule-based and AI-based detection engines.

In terms of event detection, the system must support detection of traffic surges, unauthorized access attempts, and recurring behavioral patterns using both threshold-based and policy-driven filters.

From a visualization and operations standpoint, a GUI-based monitoring system must provide intuitive displays of event timelines, device-level traffic states, and session correlations. It must also include tools for interpreting alerts and reviewing historical responses [3].

Lastly, from a policy integration and extensibility perspective, the system must provide a REST API–based interface for external integration and ensure scalability to support future AI-based detection engines and SOAR platforms [15].

These requirements not only enumerate functional needs but also serve as the foundational design criteria for building a technically viable and structurally extensible integrated security system. They inform the architecture proposed in the following chapter.

## IV. Proposed System Architecture

Based on the security requirements and structural design principles derived in the previous section, this study proposes an integrated security system architecture capable of detecting and responding to security events in real time across a converged 5G private network and enterprise network environment. The proposed system consists of five core modules: data collection, preprocessing and integration, event detection, policy-based response, and integrated monitoring. The architecture adopts a modular and lightweight design optimized for real-time responsiveness and interoperability across heterogeneous systems [4][8]. The overall flow, shown in Fig. 1, spans the full security lifecycle—collection, detection, response, and visualization.

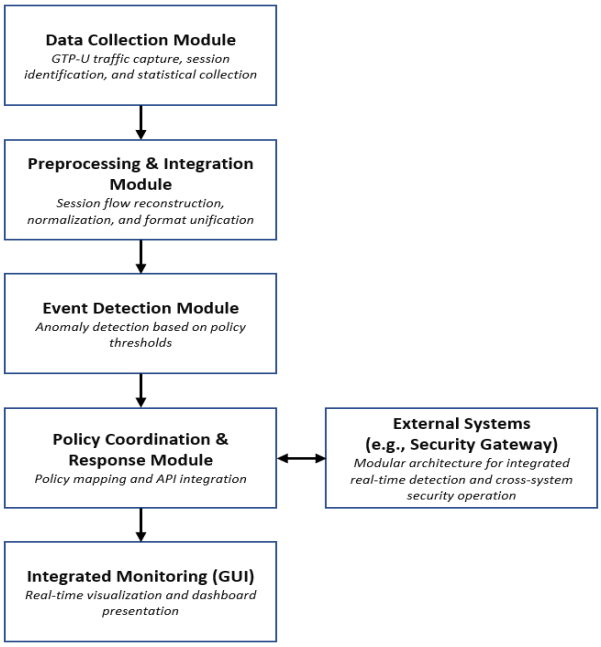


Fig. 1 Architecture of the Proposed Integrated Security System for 5G private Networks

The data collection module collects GTP-U-based user-plane traffic and control-plane logs in real time, with a fixed sampling interval of one minute. This granularity significantly improves detection sensitivity compared to conventional 15-minute intervals [2]. Collected features include device identifiers (IP, IMSI), session identifiers (TEID, Flow Label), traffic statistics (packet count, byte count), and session duration. To ensure compatibility across heterogeneous equipment, all data are normalized into a unified format [6].

The preprocessing and integration module transforms the raw data into structured inputs suitable for detection algorithms. This module performs outlier removal, missing value imputation, and normalization, followed by conversion into a flow-based statistical vector. As defined earlier in Equation (2), this vector is optimized for real-time anomaly detection [14]. A JSON-based RESTful API is also provided to ensure seamless integration and data exchange across systems, supporting syntactic and semantic interoperability between different security platforms [15].

The event detection module analyzes the preprocessed flow vectors to identify abnormal behaviors in real time. Detection criteria include unauthorized port access, sudden spikes in traffic volume, and repetitive session patterns. The detection logic is implemented using a policy-driven scenario-based filtering framework. A lightweight detection engine is employed to minimize processing delays, and the architecture is designed to be extensible, allowing for future integration with AI-based deep learning models [3].

The policy-based response module automatically applies predefined response policies according to the type of detected security event. Events are matched with corresponding response actions using an event-policy mapping table. The module is designed to interoperate with external systems such as SOAR platforms, policy servers, and gateway devices using a REST API, enabling dynamic

policy dissemination and coordinated incident response across heterogeneous infrastructures [7].

The integrated monitoring module provides a graphical user interface (GUI) that visualizes system status and detected events in real time. Key indicators such as event timelines, per-device traffic flows, and session state transitions are displayed to assist operators in tracking threat flows and conducting root cause analysis. The intuitive interface allows operators to quickly assess situations and make timely decisions [5].

Overall, the proposed system architecture goes beyond single-point detection by encompassing the entire security workflow—from data collection to detection, policy enforcement, external integration, and visualization—within a unified framework. This architecture serves as a foundational structure for future developments, including security gateway-based platforms, AI-integrated anomaly detection engines, and policy-driven SOAR coordination mechanisms [15].

## V. Application Scenarios and Evaluation Plan

To assess the design validity and practical effectiveness of the proposed integrated security system architecture, this study establishes application scenarios based on a realistic 5G private network–enterprise network integrated environment. These scenarios encompass the entire security operation flow, including real-time traffic collection, anomaly detection, policy generation, and operator observation and decision-making [2][3]. Considering the current limitation of system implementation, the scenarios are designed as simulation-based frameworks suitable for pre-deployment evaluation.

The application scenarios are categorized into two representative types. The first is a device-based anomaly detection scenario, which assumes a situation in which a specific terminal exhibits abnormal traffic behavior over a certain period (e.g., sudden surge in packet transmission or unauthorized port access). In this case, the system is expected to detect anomalies in real time, execute predefined policy-based responses, and visually deliver the results to the operator through an integrated monitoring interface [1][3].

The second is an interoperability scenario across heterogeneous security systems, wherein security events detected by different systems (e.g., firewall, IDS, policy server) are shared and integrated within the proposed architecture. This scenario focuses on evaluating whether response policies are consistently applied across different systems, beyond individual detection functionalities. It serves as a structural verification framework to assess the coordination potential of multi-system environments under policy-centric security management[6][7].

The evaluation criteria of the proposed architecture are defined as follows:

Detection Sensitivity evaluates the success rate of anomaly detection within the collection cycle upon event occurrence, quantifying the system's ability to identify abnormal behaviors.

Time-To-Detect (TTD) measures the total time from event occurrence to detection, visualization, and policy generation, serving as a key indicator for the system's real-time responsiveness [3].

System Interoperability assesses whether detected events are effectively relayed to external systems and lead to the successful execution of coordinated response actions through API-based integration [15].

Operator Visibility evaluates the intuitiveness and interpretability of event flows, session states, and traffic statistics as presented through the graphical interface, focusing on usability and situational awareness [5].

This scenario-driven evaluation framework goes beyond abstract system design by offering a concrete structure to verify practical deployability and architectural completeness in real-world conditions. Furthermore, the defined scenarios and evaluation metrics can be adopted as reference indicators in future testbed-based quantitative evaluations and platform-level security system implementations. Despite being a design-phase study, this research presents both architectural rigor and practical applicability, establishing a technical foundation for enhancing the security posture of 5G private networks.

## VI. Conclusion

This paper presented the design of an integrated security system architecture aimed at enabling real-time response to security threats in a complex network environment where 5G private networks are interconnected with enterprise networks. The proposed system consists of five core modules—data collection, preprocessing and correlation, event detection, policy-based response, and integrated monitoring—designed with a strong focus on real-time performance and interoperability across heterogeneous systems [2][3].

The structural validity of the system design was examined through two realistic application scenarios: (1) device-level anomaly detection and (2) security event coordination across heterogeneous systems. Based on these scenarios, the evaluation framework was constructed around key performance metrics such as detection sensitivity, time-to-detect (TTD), system interoperability, and operator visibility. This framework enables systematic validation of architectural feasibility and technical viability even in the pre-implementation stage [3][6].

The main contribution of this study lies in its architectural integration of real-time threat detection and policy-driven response, going beyond individual detection techniques. Notably, the incorporation of GTP-U traffic analysis, API-based system interconnection, and GUI-centric operational interfaces lays a solid foundation for future integration with SOAR platforms and AI-based detection engines [1][2][15].

Future work will focus on implementing the proposed system in a testbed environment to perform quantitative performance validation. In addition, the research will pursue policy standardization, modularization of interconnection interfaces, and integration of AI-driven threat detection models to enhance the system into a practical security platform. The proposed architecture provides a foundational framework for implementing real-time security in 5G private networks and holds promise as a core technology for advancing customized security solutions across various industrial sectors.

## ACKNOWLEDGEMENT

This work was partly supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) ( No. RS-2024-00397469, Development of Private 5G Security Technology for Integrated Private 5G and Enterprise Network Security, 100%)

## REFERENCES

[1] S. Samarakoon et al., “5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network,” arXiv preprint, arXiv:2212.01298, 2022.

[2] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “5G Core PFCP Intrusion Detection Dataset,” in Proc. of MOCAST, pp. 1‑4, 2023.

[3] P. I. Radoglou-Grammatikis et al., “5GCIDS: An Intrusion Detection System for 5G Core with AI and Explainability Mechanisms,” in Proc. of IEEE GLOBECOM Workshops, pp. 353‑358, 2023.

[4] 3GPP, "NR; Radio Resource Control (RRC); Protocol specification," 3GPP TS 38.331, Sep. 2020.

[5] J.-G. Park, Y. Kim, J.-H. Lee, J. Jang, D. Moon, and I. Kim, “5G Edge Security Technology Trends,” REVIEW OF KIISC, vol. 30, no. 6, pp. 7‑16, 2020.

[6] H. S. Park, “Survey and Study on Integration of Safety and Security in Robot Systems,” Journal of Institute of Control, Robotics and Systems, vol. 26, no. 11, pp. 988 ‑ 998, 2020. doi:10.5302/J.ICROS.2020.20.0145

[7] H. R. Oh, “A Trend on International Standardization for 5G Security in ITU-T SG17,” Proc. of the Symposium of the Korean Institute of Communications and Information Sciences, pp. 1078‑1079, 2021.

[8] H. K. Kim, “An Analysis of Trends in Overseas Security Requirements for Designing Security Technologies Suitable for 5G Structures,” REVIEW OF KIISC, vol. 30, no. 6, pp. 31‑38, 2020.

[9] J.-G. Park, J.-H. Kim, D. Moon, and I. Kim, “Features and Major Improvements of 3GPP 5G Security Structure,” REVIEW OF KIISC, vol. 29, no. 5, pp. 21‑30, 2019.

[10] T. N. Kipf and M. Welling, “Semi-Supervised Classification with Graph Convolutional Networks,” in Proc. of ICLR, 2017.

[11] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed., MIT Press, 2018.

[12] N. Moustafa and J. Slay, “The TON_IoT Datasets: A New Generation of IoT Datasets for AI-based Cybersecurity Research,” arXiv preprint, arXiv:1906.02142, 2019.

[13] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, and J. Yang, “A Survey on the Edge Computing for the Internet of Things,” IEEE Access, vol. 6, pp. 6900‑6919, 2018.

[14] M. A. Ferrag, et al., “Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study,” J. of Info. Security and Applications, vol. 54, 2020.

[15] S. S. Gill, et al., “AI for 5G Network Slicing: Requirements, Opportunities and Challenges,” IEEE Network, vol. 35, no. 2, pp. 92‑97, 2021.