JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 7, pp. 107-116, July 2026
https://doi.org/10.9708/jksci.2026.31.07.107

Research on Quantitative Security Requirements Modeling and STRM-based Architecture Mapping in ITU-T X.805 & X.1601

Gyeongsu Kim*, Hyunsu Yoo*, Hanjin Lee**

*M.S, Department of Digital Management, Korea University, Sejong, Korea
**Professor, School of Creative Convergence Education, Handong Global University, Pohang, Korea

[Abstract]

As financial institutions increasingly adopt hybrid and multi-cloud environments, the complexity of security architecture design has risen due to unclear boundaries and multi-layered data flows. Existing approaches rely heavily on expert experience and manual processes, causing inconsistencies and limited reproducibility. This study proposes a structured and quantitative methodology for deriving security requirements and mapping them to architecture design based on a unified Security Technology Reference Model (STRM) integrating standards such as ITU-T X.805 and X.1601. The model introduces a formalized Security Requirement Code (SEC) data model, a matrix-based mapping structure (Protection Object x Security Function), and a quantitative coverage metric for evaluating completeness. This proposed model improves coverage, reduces omission, and enhances design consistency.

▸ **Key words**: Security Architecture, Cloud Computing, Financial Information Security, Security Technology Reference Model, Regulatory Compliance

[요 약]

금융기관은 하이브리드 및 멀티클라우드 환경으로의 전환이 가속화됨에 따라 보안책임 경계의 불명확성과 데이터 흐름의 다계층화로 인해 보안 아키텍처 설계의 복잡성이 증가하고 있다. 기존 보안설계 방식은 전문가 경험과 수작업에 의존하는 경향이 강하여 요구사항 누락, 추적성 부족, 재현성 한계 등의 문제가 발생하고 있다. 본 연구는 ITU-T X.805와 X.1601과 같은 국제표준을 통합한 STRM(Security Technology Reference Model)을 기반으로 보안요구사항 도출과 아키텍처 설계를 통합하는 정량적 방법론을 제안한다. 제안 모델은 SEC(Security Requirement Code) 기반의 요구사항 정형화, 보호대상과 보안기능 간 매트릭스 구조, 그리고 요구사항 적용 범위를 평가하기 위한 정량적 지표를 포함한다. 금융 클라우드 환경 사례 분석 결과, 제안 방법은 요구사항 적용 범위 확대, 누락 감소, 설계 일관성 향상에 기여하는 것으로 나타났다.

▸ **주제어**: 보안 아키텍처, 클라우드 컴퓨팅, 금융 정보보호, 보안기술 참조모델, 규제 준수

• First Author: Gyeongsu Kim, Corresponding Author: Hanjin Lee
*Gyeongsu Kim (weloving@naver.com), Department of Digital Management, Korea University
*Hyunsu Yoo (n3oism@gmail.com), Department of Digital Management, Korea University
**Hanjin Lee (cus@handong.edu), School of Creative Convergence Education, Handong Global University
• Received: 2026. 04. 13, Revised: 2026. 05. 13, Accepted: 2026. 06. 17.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

디지털 전환의 가속화에 따라 금융기관의 IT 환경은 기존 온프레미스(On-premise) 중심 구조에서 하이브리드(Hybrid) 및 멀티클라우드(Multi-Cloud) 기반으로 빠르게 확장되고 있다. 이러한 환경 변화는 서비스 확장성과 운영 효율성을 향상시키는 동시에, 보안책임 경계의 모호성과 데이터 흐름의 다계층화로 인해 기존 보안설계 방식의 한계를 더욱 분명하게 드러내고 있다 [1-5]. 특히 금융기관은 전자금융감독규정, 개인정보보호법, 신용정보법, ISMS-P, ISO/IEC 27001과 같은 다층적 규제를 동시에 준수해야 하며, 최근 금융분야 클라우드 이용 가이드와 상용 클라우드 보안관리 참고서, 그리고 클라우드 보안인증 및 취약점 점검 가이드와 같은 실무 지침도 함께 고려해야 한다 [6-10]. 이 때문에 보안설계는 단순한 기술 구현을 넘어 규제 준수와 직결되는 핵심 설계요소로 작용한다.

그러나 실제 현업에서는 보안요구사항 도출과 아키텍처 설계가 여전히 전문가의 경험과 수작업 중심으로 수행되는 경우가 많으며, 이로 인해 요구사항의 누락, 중복, 해석 편차가 지속적으로 발생하고 있다 [11-15]. 이러한 문제는 보안설계의 일관성과 재현성을 저해할 뿐 아니라, 규제 대응 과정에서도 반복적인 문서 수정과 검토 부담을 유발한다.

기존 연구들은 규제 분석, 보안 프레임워크, 클라우드 보안기술을 개별적으로 다루는 경향이 있으며, 보안요구사항 도출에서 아키텍처 설계까지 통합적으로 연결하는 구조화된 방법론은 상대적으로 부족하다 [16,17]. 특히 ITU-T X.1601과 X.805, 그리고 Zero Trust Architecture와 같은 대표적 참조모델은 보안구조를 설명하는 데 유용하지만, 금융권 규제 요구사항을 정량적으로 구조화하여 실제 아키텍처 설계로 연결하는 절차까지 직접 제공하지는 않는다 [16-18].

국내외 관련 연구에서도 안전한 클라우드 보안 아키텍처, X.805 기반 프레임워크 도출, AWS 보안 서비스 적용, PCI DSS와 같은 컴플라이언스 요구사항, Zero Trust 기반 트래픽 제어 및 정책 기반 접근제어 기법, 그리고 금융 규제와 클라우드 법제도 개선방안이 각각 제시되어 왔으나, 이들 연구는 규제, 구조, 통제, 기술 구현을 하나의 설계 절차 안에서 정량적으로 통합하지는 못하였다 [19-25]. 이에 본 연구는 ITU-T X.805와 X.1601을 통합한 STRM (Security Technology Reference Model)을 기반으로 보안요구사항을 정형화하고, 보호대상과 보안기능 간 매핑 구조를 통해 요구사항과 아키텍처 간의 관계를 체계적으로 정의하는 정량적 모델을 제안한다.

II. Theoretical Background and Related Works

기존 연구는 보안요구사항 도출 및 아키텍처 설계 관점에서 규제 및 표준 기반 접근, 보안 프레임워크 기반 접근, 그리고 클라우드 보안기술 중심 접근으로 구분할 수 있다. 규제 및 표준 기반 접근은 금융권 보안위협과 요구사항, 모바일 전자금융서비스 보안성 검토, 금융분야 클라우드 이용규제, 그리고 클라우드 서비스 정보보호 프레임워크와 같은 연구에서 확인되듯이 규제 준수 측면에서는 유용하지만, 실제 시스템 설계와의 연계성은 제한적인 경우가 많다 [1,11-14].

보안 프레임워크 기반 접근은 ITU-T X.1601과 X.805, 그리고 Zero Trust Architecture와 같이 보안구조를 설명할 수 있는 이론적 틀을 제공한다는 장점이 있다. 그러나 X.805는 전통적 네트워크 중심 구조에 강점을 가지는 반면 클라우드 반영이 부족하고, X.1601은 클라우드 환경에 적합하지만 온프레미스와의 통합적 설계 관점은 상대적으로 제한적이다 [16-18,20]. 국내에서도 안전한 클라우드 컴퓨팅 환경을 위한 보안 아키텍처 연구와 X.805 기반 정보보호 프레임워크 도출 연구가 수행되었으나, 규제 요구사항을 정량적으로 구조화하여 설계 단계로 연결하는 수준까지는 확장되지 않았다 [19,20].

클라우드 보안기술 중심 접근은 AWS 보안 서비스 활용, PCI DSS 준수, AWS 보안 아키텍처 구성, REST 기반 보안 프레임워크, 그리고 클라우드 환경에서의 Zero Trust 구현과 같은 연구에서 확인되듯이 운영 및 구현 단계에서 실질적인 통제 방안을 제시한다 [15,21-23]. 다만 이러한 접근은 주로 특정 환경 또는 기술 요소에 초점을 맞추고 있어, 규제 요구사항 자체를 정형화하고 이를 설계 구조로 일관되게 변환하는 체계를 충분히 제공하지는 않는다.

또한 클라우드 관련 연구 중에는 거버넌스, 법·제도 개선 및 규제 체계에 대한 연구도 수행되고 있으며, 이러한 연구는 클라우드 환경에서의 정책적·관리적 관점을 제공한다 [24,25]. 그러나 최근 연구에서는 클라우드 거버넌스와 규제 체계, 보안 아키텍처 적용 방법론에 대한 논의가 확

대되고 있으나, 요구사항과 설계 간 정량적 연결 구조를 제시하는 연구는 여전히 제한적이다 [24-26].

이러한 선행연구를 종합하면, 보안요구사항과 아키텍처 설계 간의 구조적 연결 부족, 요구사항의 데이터 기반 관리 체계 부재, 그리고 보안통제 적용 범위에 대한 정량적 평가 부족이 공통적인 한계로 도출된다.

나아가 CSA Cloud Controls Matrix(CCM), NIST SP 800-53, NIST Cybersecurity Framework (CSF), ISO/IEC 27002, CIS Controls, SABSA 및 TOGAF Security Architecture와 같은 대표적인 보안 프레임워크는 통제 항목 체계 또는 보안 아키텍처 원칙을 제공한다는 장점이 있다.

하지만 이들 프레임워크는 규제 요구사항을 정형화된 데이터 객체로 구조화하고, 이를 보안 아키텍처 설계와 정량적으로 연결하기 위한 절차를 직접 제공하지는 않는다.

반면 본 연구는 STRM을 기반으로 보안요구사항을 SEC(Security Requirement Code) 모델로 정형화하고, 보호대상과 보안기능 간 매핑을 통해 요구사항부터 보안통제 및 아키텍처 설계까지의 추적성을 확보한다는 점에서 기존 프레임워크와 차별성을 가진다. 즉, Coverage 기반 정량 평가를 통해 보안요구사항 적용 범위를 분석할 수 있다는 점에서도 기존 접근 방식과 차별화된다.

이번 연구에서는 이러한 한계를 보완하기 위해 STRM 기반의 정량적 보안요구사항 모델과 아키텍처 매핑 절차를 제안한다.

Table 1. Comparison of Security Architecture Approaches

Category	ITU-T X.805	ITU-T X.1601	Zero Trust Architecture	Proposed STRM
Primary Scope	On-Premises Infrastructure	Cloud Computing Environment	Access Control and Identity-Centric Security	Integrated Hybrid Environment
Requirement Formalization	Not Provided	Not Provided	Not Provided	Provided
Quantitative Assessment	Not Supported	Not Supported	Not Supported	Supported
Requirement-to-Architecture Traceability	Limited	Limited	Limited	Supported

앞서 탐구한 CSA CCM, NIST SP 800-53과 같은 프레임워크도 검토하였으나, 본 연구의 목적이 보안통제 체계 수립이 아닌 요구사항과 아키텍처 간 정량적 매핑 모델 제안에 있으므로 비교 대상은 보안 아키텍처 관점에서 직접적인 관련성이 높은 X.805, X.1601 및 Zero Trust Architecture를 중심으로 구성하였다.

요컨대 기존 접근과 달리 보안요구사항을 SEC 모델로 정형화하고, STRM 기반 매트릭스를 통해 요구사항과 아키텍처 간 관계를 정량적으로 정의함으로써 설계의 일관성과 재현성을 확보하는 것을 목표로 한다.

III. STRM-based Quantitative Security Requirements Model

제안하는 연구에서는 ITU-T X.805와 X.1601의 구조적 강점을 결합하여 STRM을 정립하고자 한다. X.805는 End-to-End 보안관점에서 계층과 보안기능 차원을 체계화한 반면, X.1601은 클라우드 환경의 책임분담과 가상화 특성을 반영한다. STRM은 두 표준을 통합하여 내부 인프라와 클라우드가 혼재된 환경에서도 일관된 보안설계를 가능하게 하는 참조 구조를 제공한다.

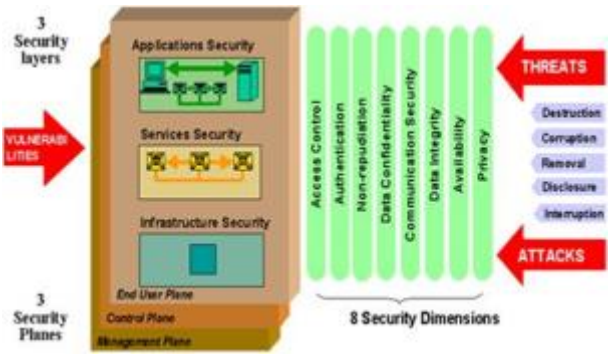

Fig. 1. ITU-T X.805 Security Architecture

그림1(Figure 1)은 ITU-T X.805에서 정의한 보안 아키텍처를 나타내며, 보안 계층(Security Layer), 보안 차원(Security Dimension) 및 종단간 통신 관점(End-to-End Communication)을 기반으로 보안요구사항을 구조화한다.

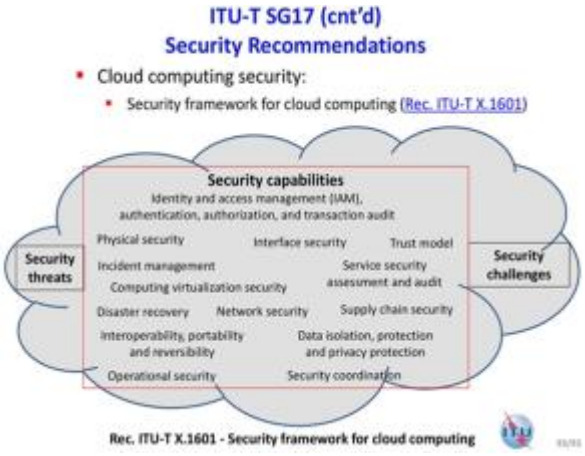

Fig. 2. ITU-T X.1601 Cloud Security Architecture

다음의 그림2(Figure 2)는 ITU-T X.1601에서 정의한 클라우드 보안 아키텍처를 나타내며, 클라우드 서비스 모델과 책임분담 구조를 기반으로 보안 요구사항을 정의한다.

Table 2. Comparison Between ITU-T X.805 and X.1601

Category	ITU-T X.805	ITU-T X.1601
Primary Scope	Telecommunication Networks and On-Premises Systems	Cloud Services (IaaS / PaaS / SaaS)
Architectural Perspective	Layer- and Dimension-Based Security Architecture	Service Model and Virtualization-Oriented Security Architecture
Strengths	Clear End-to-End Security Structuring and Explicit Layer Interdependencies	Explicit Shared Responsibility Model, Virtualization Security, and Data Sovereignty Considerations
Limitations	Limited Consideration of Cloud-Native and Virtualized Environments	Insufficient Integration with On-Premises Infrastructure and Traditional Network Security
Complementarity	Provides Fundamental Security Principles for Traditional Infrastructure	Provides Cloud-Specific Security Controls → Combined Use Enables Comprehensive Coverage of Hybrid Environments

STRM의 핵심 개념은 전체 보안체계를 '보호대상(Protection Object)'과 '보안통제(Security Function)'의 관계로 구조화하는 것이다. 먼저 보호대상은 데이터 흐름에 따라 단말기(Endpoint), 네트워크(Network), 서버(Server), 애플리케이션(Application), DBMS, 클라우드(Cloud)로 구분된다. 다음으로 보안통제는 접근통제(Access Control), 식별 및 인증(Identification and Authentication), 권한관리(Authorization Management), 기밀성(Confidentiality), 개인정보보호(Privacy Protection), 무결성(Integrity), 가용성(Availability), 로깅 및 감사(Logging and Audit Trail), 보안운영(Security Operations and Management)로 정규화된다(Figure 3).

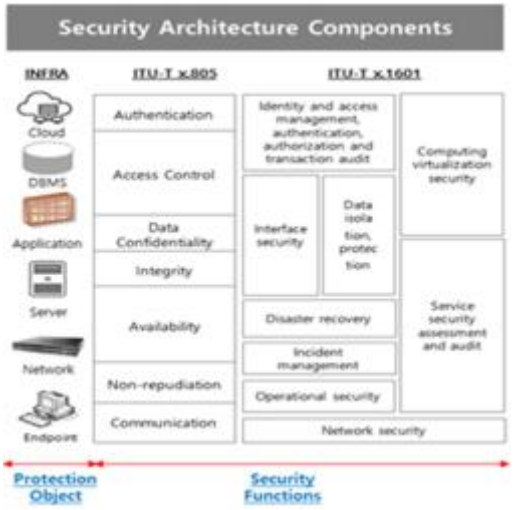

Fig. 3. STRM Components and Structure

그림4(Figure 4)는 제안하는 STRM의 핵심 구조를 나타낸다. STRM은 ITU-T X.805와 ITU-T X.1601의 보안 기능을 통합하고, 이를 보호대상(Protection Object)과 연계하여 표현한다. 보호 대상은 Endpoint, Network, Server, Application, DBMS, Cloud로 구성되며, 이를 통해 보안요구 사항 도출과 아키텍처 설계 간의 추적 가능한 관계를 정의할 수 있다. 또한 STRM은 본 연구에서 제안하는 SEC 기반 보안요구사항 모델링과 정량적 매핑 절차의 기반 구조로 활용된다.

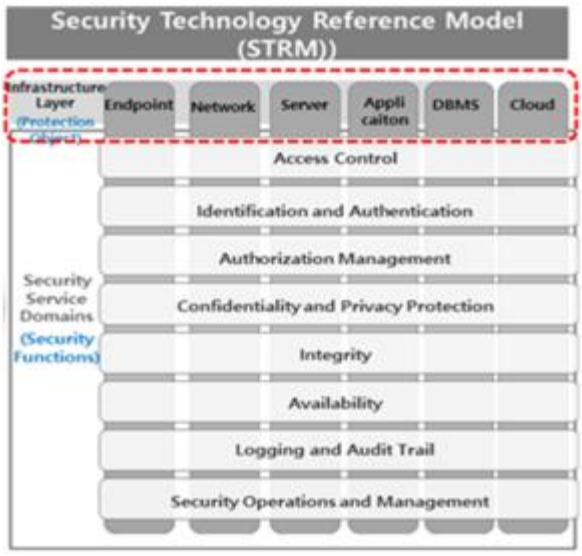

Fig. 4. STRM Matrix Structure (Protection Object × Security Function)

본 구조는 ITU-T X.805와 X.1601을 통합하여 보호대상과 보안기능 간 매트릭스 관계를 정의한 연구자의 제안 모델이다. 이는 STRM의 핵심 분석 구조로서 보안요구사항 분류, Coverage 기반 정량 평가 및 보안 아키텍처 매핑의 기준으로 활용된다. 게다가 요구사항과 설계요소 간 추적성을 확보하기 위한 참조모델 역할을 수행한다.

이 두 요소를 매트릭스 형태로 대응시킴으로써, 각 인프라 계층에 적용되어야 할 보안요구사항을 위치 기반으로 식별할 수 있으며, 통제의 누락·중복 여부를 구조적으로 검증할 수 있다. 이는 보안설계를 문서 작업이 아닌 데이터 기반 구조설계 문제로 전환하는 핵심적 특징이다.

IV. Security Requirements Derivation and Architecture Design Procedure

본 연구는 기존 보안설계가 전문가 경험과 비정형 문서에 의존함으로써 발생하는 요구사항 누락, 중복 및 적용 불일치 문제를 해결하기 위해, 보안요구사항 도출부터 아키텍처 설계까지를 하나의 구조화된 절차로 정의한다.

이에 제안하는 절차는 STRM을 중심으로 보안요구사항을 정형화하고, 보호대상과 보안기능 간 매핑을 통해 요구사항을 아키텍처 설계로 연결하는 것을 목표로 한다.

1. Derivation of Security Requirements Based on Regulations and Standards

보안요구사항 도출 단계에서는 전자금융감독규정, 개인정보보호법, 신용정보법, ISMS-P, ISO/IEC 27001 등 금융권 주요 규제 및 국제표준을 분석 대상으로 설정하였다.

각 규제 문서는 조항 단위로 분해한 후, 선언적 표현을 기술적 요구사항으로 재해석하여 보안요건으로 정제하였다. 이 과정에서 중복되거나 추상적인 표현은 통합하여 실제 시스템 설계에 적용 가능한 수준으로 구체화하였다.

도출된 보안요구사항은 SEC(Security Require ment Code) 모델을 기반으로 정형화되며, 각 요구사항에는 고유 식별자를 부여하여 데이터 기반 관 리가 가능하도록 하였다.

Table 3. Structure of Security Requirement Definition(SEC Data Model)

No.	Field	Description
①	SEC Code	Unique identifier assigned to each security requirement (e.g, SEC-030).
②	Requirement Name	Concise title summarizing the core intent of the security requirement (e.g., Encryption of Sensitive Data).
③	Requirement Definition	Refined requirement statement derived from legal, regulatory, and international standard provisions, translated into technical and implementable terms.
④	Classification Criterion	Security control category based on STRM Security Functions, indicating the relevant security service domain (e.g., Access Control, Authentication, Confidentiality).
⑤	Applicable Target	Infrastructure classification based on STRM Protection Objects, identifying the infrastructure layers where the requirement must be applied (e.g., Endpoint, Server, Cloud).
⑥	Related Regulations and References	Applicable laws, supervisory regulations, and standard clause identifiers supporting the requirement.
⑦	Verification Evidence	Types of evidence used to verify implementation, such as logs, configuration values, inspection reports, or audit records.
⑧	Implementation Priority	Priority level of the requirement (High / Medium /Low) or indication of mandatory compliance status.
⑨	Remarks / Change History	Management metadata including revision date, related systems, responsible personnel, and change history.

표 3(Table 3)는 보안요구사항을 정형화된 데이터 객체로 정의한 구조를 나타내며, 요구사항의 추적성과 재사용성을 확보하기 위한 기반을 제공한다.

2. Classification and Structuring of Security Requirements Based on STRM

정형화된 보안요구사항은 STRM의 핵심 구성요소인 보호대상(PO)과 보안기능(SF)을 기준으로 분류 된다. 먼저 보호대상은 Endpoint, Network, Server, Application, DBMS, Cloud로 구분되며, 보안기능은 접근통제부터 보안운영까지 정의된다.

각 SEC 코드는 하나 이상의 보호대상 및 보안기능에 매핑되며, 이를 통해 보안요구사항의 적용 범위와 성격을 구조적으로 정의할 수 있다.

Table 4. SEC Code Application by Protection Object

Security Requirement Name	Common SEC Code	Endpoint (C)	Network (N)	Server (S)	Application (A)	DBMS (D)	Cloud (V)	Generated Detailed SEC Codes
Encryption of Sensitive Data	SEC-030	●			●	●	●	SEC-030 (C/A/D/V)
Access Endpoint Restriction	SEC-012	●	●	●	●	●	●	SEC-012 (C/N/S/A/D/V)

● : Applicable to the corresponding Protection Object, Blank : Not applicable

표 4(Table 4)는 보안요구사항이 보호대상별로 어떻게 확장 및 적용되는지를 나타내며, 요구사항의 적용 범위를 구조적으로 식별할 수 있도록 한다.

3. Quantification and Mapping Procedure of Security Requirements

STRM 기반 매핑 단계에서는 보안요구사항의 적용 여부를 보호대상과 보안기능 간 관계로 정의한다. 이 관계는 다음과 같은 매핑 함수로 표현된다.

$$M(PO,\ SF) \in \{0,1\}$$

여기서 1은 해당 보안통제가 적용됨을 의미하며, 0은 적용되지 않음을 의미한다. 이를 통해 보안요구사항은 매트릭스 형태로 표현되며, 각 요구사항의 적용 범위를 정량적으로 분석할 수 있다.

나아가 보안요구사항 적용 범위는 다음과 같이 정의된다.

$$Coverage = (적용된\ 보안통제\ 수 \\ /\ 적용이\ 필요한\ 전체\ 보안통제\ 수)$$

이 구조를 통해 요구사항 누락 여부를 체계적으로 식별할 수 있으며, 설계의 일관성을 정량적으로 평가할 수 있다.

다음은 STRM 기반 보안기능과 보호대상 간 매핑 구조를 나타낸다.

Table 5. STRM Matrix: Mapping Between Security Functions and Protection Objects

Protection Object → / Security Function ↓	Endpoint	Network	Server	Application	DBMS	Cloud
Access Control	●	●	●	●	●	●
Identification and Authentication	●	○	●	●	●	●
Authorization Management	○	●	●	●	●	●
Confidentiality	●	●	●	●	●	●
Privacy Protection	●	○	●	●	●	●
Integrity	○	○	●	●	●	●
Availability	○	●	●	●	●	●
Logging and Audit Trail	●	●	●	●	●	●
Security Operations and Management	○	○	○	○	○	●

Legend:
● : Applicable, ○ : Not applicable

본 매트릭스(Table 5)는 보안기능과 보호대상 간 적용 관계를 정량적으로 표현하며, 보안요구사항 적용 범위를 분석하기 위한 기준을 제공한다.

4. Mapping to Security Architecture Design

나아가 정량화된 보안요구사항은 다음과 같은 변환 함수에 의해 아키텍처 설계 요소로 연결된다.

$$Security\ Control = f(SEC,\ PO,\ SF)$$

이를 통해 각 보안요구사항은 특정 인프라 계층에서 요구되는 보안통제로 변환되며, 설계 과정에서 일관된 적용이 가능해진다. 특히 클라우드 환경에서는 책임분담 모델을 고려하여 CSP와 사용자 영역을 구분하고, 각 영역에 적합한 보안통제를 적용한다.

이 변환 함수는 보안요구사항을 단순 개념 수준에서 실제 설계요소로 연결하는 핵심 메커니즘으로, 동일한 SEC 코드라도 보호대상과 보안기능의 조합에 따라 서로 다른 보안통제로 구체화될 수 있다. 이를 통해 보안설계는 기술 선택이 아닌 구조적 매핑 과정으로 전환된다.

Table 6. Mapping of Security Controls with STRM

Security Function / Protection Object	End point	Network	Server	Appli-cation	DBMS	Cloud
Access Control	MDM, EDR	VPN, NAC, Firewall	PAM, Active Directory	Web Applic ation Server ACL	Database Access Control	IAM, Security Groups
Identification and Authentication	OTP, FIDO	VPN Authenti cation	PAM, OS Login	SSO, Token-based Authen tication	Database Authen-tication	IAM, STS
Authorization Management	DRM, DLP	NAC Policy	RBAC, OS Groups	Role-Based Access Control	Database Roles	IAM Policies
Confidentiality	Disk Encry-ption	TLS	File Encryp tion, SSL	HTTPS, Secure Cookies	Column -level Encryp tion	KMS, Secrets Manager
Privacy Protection	DRM, Data Masking	Secure Channels	OS-level Encryp tion	API Masking	Data Masking	Cloud DLP
Integrity	MDM Integrity Check	IPS, IDS	Hash Verifi-cation	Code Signing	Database Integrity Check	Cloud Config uration Control
Availability	End point Redun-dancy	L4/L7 Load Balancer	Cluster -ing	WAS Auto Scaling	Database Replica-tion	Cloud Auto Scaling
Logging and Audit Trail	Local Logs	NMS, Syslog	OS Syslog	Applic ation Logs, Audit Trails	Database Audit Logs	Cloud Trail, Configu-ration Logs
Security Operations and Management	Patch Manag ement Agent	Network Manage ment System	Vulner ability Scanner	DevSec Ops Security Tools	Database Monitor-ing	CSPM, CNAPP

표 6(Table 6)은 STRM 기반 매핑 결과를 실제 보안통제 구현 요소로 변환한 예시로, 요구사항이 아키텍처 설계로 연결되는 과정을 보여준다.

5. Procedural Implications

본 절에서 제시한 절차는 보안요구사항을 단순 문서가 아닌 구조화된 데이터로 전환하고, 이를 아키텍처 설계에 직접 활용할 수 있도록 한다는 점에서 의의를 가진다. 이를 통해 보안설계는 경험 기반 접근에서 벗어나, 재현성과 일관성을 갖는 구조 기반 설계 방식으로 전환될 수 있다.

V. Case Study and Validation

이번 연구에서 제안한 STRM 기반 보안요구사항 정량화 및 아키텍처 매핑 모델의 타당성을 검증하기 위해, 금융기관 하이브리드·멀티클라우드 환경 구축 프로젝트 사례를 대상으로 적용 및 분석을 수행하였다. 크게 검증은 정량적 평가와 정성적 평가를 병행하는 방식으로 수행하였다.

대표적으로 살펴볼 사례는 국내 금융기관의 차세대 시스템 구축 사업 중 하이브리드·멀티클라우드 환경 적용 프로젝트를 대상으로 수행하였다. 분석 대상은 프로젝트 범위 정의서, 보안요구사항 정의서, 보안성 검토 결과서 및 보안 아키텍처 설계서이며, 동일 프로젝트를 기준으로 기존 방식과 STRM 기반 방식을 비교분석했다. 평가 과정에서는 제안된 기준에 따라 보호대상과 보안기능 간 매핑을 수행하고, 프로젝트 범위에 해당하는 보안통제의 적용 여부를 확인하였다.

1. Design of Quantitative Validation

앞서 밝힌 바와 같이, 본 연구에서는 STRM(Security Technology Reference Model) 기반 보안요구사항 정량화 모델의 적용 효과를 분석하기 위해 보안요구사항 적용 범위를 나타내는 Coverage 지표를 활용하였다. Coverage는 보호대상과 보안기능 간 매핑 결과를 기반으로 적용된 보안통제의 비율을 측정하는 지표로서 정의한다.

다만 여기에서 Coverage는 보안통제의 강도, 성숙도 또는 보안성 수준을 평가하기 위한 지표가 아니라, 보안요구사항이 설계 과정에 얼마나 충실하게 반영되었는지를 평가하기 위한 요구사항 적용 범위 지표로 정의하였다.

적용이 필요한 전체 보안통제 수는 STRM에서 정의한 6개의 보호대상(Endpoint, Network, Server, Application, DBMS, Cloud)과 9개의 보안기능의 조합을 기준으로 산정하였다. 이에 따라 전체 통제 후보군은 최대 54개(6×9) 항목으로 구성된다. 이 중 실제 프로젝트 범위에 해당하는 통제만을 평가 대상으로 선정하였으며, 선정 여부는 프로젝트 범위 정의서, 보안요구사항 정의서, 보안성 검토 결과서 및 보안 아키텍처 설계서를 기준으로 판단하였다.

모든 보안통제에 동일 가중치를 적용하였으며, 통제 중요도, 위험도 또는 규제 영향도에 따른 별도의 가중치는 부여하지 않았다. 이는 본 연구의 목적이 개별 보안통제의 우수성을 평가하는 것이 아니라, 요구된 보안통제가 설계 과정에 누락 없이 반영되었는지를 정량적으로 확인하는 데 있기 때문이다.

따라서 해당 지표는 인프라 계층 전반에 걸친 보안요구사항 적용의 일관성을 평가하고, 누락된 보안통제를 식별하기 위한 정량적 기준으로 활용된다. 즉, 금융기관의 하이브리드·멀티클라우드 구축 프로젝트를 대상으로 기존 전문가 중심 설계 방식과 STRM 기반 설계 방식의 Coverage 수준을 비교 분석하여 제안 모델의 적용 효과를 검증하였다.

2. Results of Quantitative Validation

사례 분석 결과, STRM 기반 접근 방식은 기존 방식 대비 보안요구사항 적용 범위가 확장되는 경향을 보였으며, 요구사항 누락 감소 및 설계 일관성 측면에서 개선효과가 관찰되었다.

특히 STRM 매트릭스를 활용한 구조적 매핑을 통해, 기존 방식에서 일부 누락되었던 보안통제가 체계적으로 식별되는 것으로 나타났다.

Table 7. Quantitative Comparison of Coverage and Design Quality between Conventional and STRM -based Approaches

Category	Conventional Approach	STRM-based Approach
Evaluated Security Controls	47	47
Applied Security Controls	28	43
Coverage Level	59.6%	91.5%
Requirement Omission	Partially Observed	Structurally Minimized
Design Consistency	Dependent on Individual Experience	Rule-based Consistency
Requirement Traceability	Limited	Explicitly Established

* Evaluation Criteria:
- Implemented security control = 1
- Non-implemented security control = 0
- Coverage = Number of implemented security controls / Total number of evaluated security controls

여기에서 Coverage는 보안통제의 품질 수준을 의미하는 것이 아니라, 설계 과정에서 요구된 통제가 실제로 반영되었는지를 측정하기 위한 적용 범위 지표이다. 본 사례에서는 STRM 기준에 따라 총 54개의 보안통제 후보군을 식별하였다. 이 중 프로젝트 범위에 해당하는 47개 통제를 평가 대상으로 선정하였으며, 평가는 프로젝트 설계 산출물 및 보안성 검토 결과를 기준으로 수행하였다.

기존 방식에서는 47개 통제 중 28개 통제가 설계 산출물에 반영되어 Coverage 59.6%를 나타냈다. 반면 STRM 기반 방식에서는 동일 조건에서 43개 통제가 반영되어 Coverage 91.5%를 기록하였다. 특히 접근통제, 로깅 및 감사, 보안운영 영역에서 기존 방식에서 누락되었던 요구사항이 추가로 식별되었으며, 이를 통해 요구사항 적용 범위가 확대되는 결과를 확인하였다.

특히 접근통제, 로깅 및 감사(Logging and Audit Trail), 보안운영 영역에서 기존 방식은 담당자 경험에 따라 적용 여부가 달라지는 경향이 있었으나, STRM 기반 접근 방식에서는 보호대상과 보안기능 간 매핑 규칙에 따라 일관성 있게 적용되었다.

더불어 요구사항과 보안통제 간 관계가 명확하게 정의됨에 따라 설계 변경 시 영향도 분석이 용이해졌으며, 규제 대응 과정에서 요구사항 추적성(Traceability) 확보에도 긍정적인 효과가 확인되었다. 따라서 STRM 기반 접근 방식은 단순한 Coverage 향상뿐 아니라 보안요구사항 누락 감소, 설계 일관성 확보 및 규제대응 효율성 향상 측면에서도 유의미한 개선효과를 제공하는 것으로 분석되었다.

요컨대 본 연구는 복수의 금융기관 프로젝트 적용 경험을 기반으로 방법론을 설계하고 검증하였다. 다만 금융권 중심 사례를 대상으로 분석이 수행되었으므로, 향후 공공·제조·의료 등 다양한 산업 환경에 대한 추가 검증을 통해 일반화 가능성을 확대할 필요가 있다.

3. Design of Qualitative Validation

한편 정성적 검증은 금융기관 클라우드 구축 및 보안 아키텍처 설계 경험을 보유한 전문가를 대상으로 수행하였다.

평가 대상은 금융회사 정보보호 담당자 1명, 본 사례 프로젝트에 참여한 보안 아키텍트 1명, 그리고 금융권 보안 아키텍처 구축 및 정보보호 컨설팅 경험을 보유한 정보보호 전문가 2명 등 총 4명으로 구성하였다. 이 중 정보보호 전문가 2명은 금융권 보안 아키텍처 구축 경험을 바탕으로 실무 협의 및 전문가 자문 형태로 의견을 제공하였다.

의견 수집은 이메일 질의응답과 전문가 인터뷰를 병행하여 수행하였다. 금융회사 정보보호 담당자와 프로젝트 참여 보안 아키텍트는 이메일을 통해 의견을 수집하였으며, 정보보호 전문가 2명은 실무 협의 과정에서 수행된 전문가 인터뷰를 통해 의견을 수집하였다.

평가 항목은 보안요구사항 추적성(Requirement Traceability), 설계 일관성(Design Consistency), 규제 대응 용이성(Regulatory Compliance Support), 요구사

항 누락 감소(Reduction of Requirement Omission)의 4개 영역으로 구성하였다. 수집된 의견은 공통 응답 내용을 중심으로 분석하였으며, STRM 기반 접근 방식과 기존 방식 간 차이에 대한 정성적 평가를 수행하였다.

분석 결과, 참여자들은 STRM 기반 접근 방식이 기존의 경험 중심 설계 대비 요구사항과 설계 간 연결성을 향상시키고 규제 대응 과정에서 설명 가능성과 추적성을 높이는 데 도움이 된다고 평가하였다. 특히 보안요구사항과 설계 요소 간 관계가 명확하게 정의됨에 따라 보안성 심의 대응과 변경 영향도 분석이 용이해졌으며, 설계 단계에서 누락될 수 있는 보안요구사항을 보다 체계적으로 식별할 수 있다는 의견이 공통적으로 제시되었다.

다만 본 정성적 평가는 제한된 수의 전문가를 대상으로 수행되었으므로, 향후 다양한 산업군과 프로젝트를 대상으로 추가적인 검증이 필요하다.

4. Summary of Validation Results

정량적 검증과 정성적 검증 결과를 종합하면, STRM 기반 방법론은 보안요구사항 적용 범위 향상, 설계 일관성 확보, 규제 대응 효율성 개선이라는 측면에서 의미 있는 개선효과가 확인되었다.

물론 본 연구의 정량적 검증은 단일 사례 기반으로 수행되어 한계가 있으므로, 다양한 환경에 대한 추가적인 검증이 필요하다. 여기서 제안한 Coverage 지표는 요구사항 적용 여부를 중심으로 한 기초 정량화 모델에 해당하기 때문이다. 따라서 모든 보안통제에 동일 가중치를 적용하였으며, 통제 중요도 또는 위험도를 반영하지 못한 한계점이 존재한다.

이에 향후 연구에서는 금융규제 영향도, 보안위험도 및 통제 중요도를 반영한 가중치 기반 Coverage 모델을 개발함으로써 보다 정교한 정량 평가 체계로 확장할 필요가 있다.

VI. Conclusion

본 연구는 국제표준 기반 STRM(Security Technology Reference Model)을 활용하여 보안요구사항 도출과 아키텍처 설계를 통합하는 정량적 모델을 제안하였다. 보안요구사항을 SEC(Security Requirement Code) 모델로 정형화하고, 보호대상과 보안기능 간 매핑 구조를 통해 요구사항과 아키텍처 간의 관계를 체계적으로 정의함으로써 기존의 경험 기반 보안설계 방식이 지닌 한계를 보완하였다.

선행연구와 사례 분석을 종합하면, 기존 접근은 규제 중심, 프레임워크 중심, 기술 중심으로 분절되어 있었으며, 이로 인해 요구사항과 설계 간의 직접적인 연결성과 재현성이 충분히 확보되지 못하였다 [1, 14-18, 21-25]. 이에 비해 STRM 기반 접근은 보안요구사항을 구조화된 데이터 객체로 관리하고, 인프라 계층과 보안기능 간의 매핑을 통해 설계의 일관성과 추적성을 강화한다는 점에서 차별성을 가진다. 또한 AWS 중심의 구현 사례와 클라우드 컴플라이언스 및 보안 거버넌스 관련 연구를 함께 고려할 때, 본 연구가 제안하는 방법론은 특정 기술이나 CSP에 종속되지 않는 확장 가능한 설계 프레임워크로 활용될 수 있다 [21-25].

후속 연구에서는 다양한 산업 환경과 다수의 프로젝트를 대상으로 정량적 검증을 확대하고, STRM 기반 모델을 AI 기반 자동 설계 및 DevSecOps 환경과 연계하여 발전시키는 방향이 필요하다.

REFERENCES

[1] D. Shin, I. Yoo, and J. Kim, “A Study on Cloud Security Threats and Security Requirements in the Korean Financial Sector,” Journal of the Korea Next-Generation Computing Society, vol. 20, no. 4, pp. 77-96, 2024. doi:10.23019/kingpc.20.4.202408.007

[2] J. S. Lim, “A Study on Security Policies for Activating Cloud Adoption in Financial Companies,” Journal of Culture Technology, vol. 3, no. 4, pp. 199-205, 2017. doi:10.17703/JCCT.2017.3.4.199

[3] K. N. Mishra, V. Bhattacharjee, S. Saket, and S. P. Mishra, “Cloud and Big Data Security System’s Review Principles: A Decisive Investigation,” Wireless Personal Communications, vol. 117, no. 2, pp. 1-38, 2022. doi:10.1007/s11277-022-09781-0

[4] M. Hossain, G. Kayas, R. Hasan, A. Skjellum, S. Noor, and S. M. R. Islam, “A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives,” Future Internet, vol. 16, no. 2, Art. 40, 2024. doi:10.3390/fi16020040

[5] S.-J. Park, Y.-J. Lee, and W.-H. Park, “Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network,” Security and Communication Networks, vol. 2022, Art. 3686423, 2022. doi:10.1155/2022/3686423

[6] Financial Security Institute, Guide to the Use of Cloud Computing Services in the Financial Sector (2025 Revision), Seoul, Korea, 2025.

[7] Financial Security Institute, Reference Guide for Security Management of Commercial Cloud Services in the Financial Sector, Seoul, Korea, 2024.

[8] Korea Internet & Security Agency, Guide to Cloud Service (IaaS) Security Certification Criteria (ISMS-P/CSAP), Naju, Korea, 2024.
[9] Korea Internet & Security Agency, Guide to Cloud Vulnerability Assessment (ISMS), Naju, Korea, 2024.
[10] J. Bae and S. Lee, "Legal Regulations on the Use of Cloud Computing Services by Financial Companies," Law Firm Kwangjang Issue Paper, 2020.
[11] H. S. Yoo, J. D. Kim, and S. J. Kim, "A Study on Improving Security Inspection Items for Security Review of Mobile Electronic Financial Services," Journal of Industrial Security, vol. 7, no. 1, pp. 129-158, 2017.
[12] M. Kim, "Regulation and Improvement Measures for the Use of Cloud Services in the Financial Sector," in Proceedings of the 2020 Spring Conference of the Korea IT Service Society, pp. 413-416, 2020.
[13] H. Park, "A Phenomenological Study on Shoulder Surfing Experience in Mobile Financial Service Use," in Proceedings of the 2023 Conference of the Korean Society of Design, pp. 176-181, 2023.
[14] C.-W. Lee and K.-W. Park, "A Study on Information Security Framework for Cloud Services: Focusing on Security Requirements," in Proceedings of the 2021 Spring Conference of the Korea Next-Generation Computing Society, pp. 337-340, 2021.
[15] J. Singh and N. K. Chaudhary, "REST Security Framework for Event Streaming Bus Architecture," International Journal of Information Technology, vol. 16, no. 5, pp. 3033-3047, 2024. doi:10.1007/s41870-024-01836-8
[16] International Telecommunication Union, Security Framework for Cloud Computing (Recommendation ITU-T X.1601), Geneva, Switzerland, 2015.
[17] International Telecommunication Union, Security Architecture for Systems Providing End-to-End Communications (Recommendation ITU-T X.805), Geneva, Switzerland, 2003.
[18] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. doi:10.6028/NIST.SP.800-207
[19] S.-Y. Choi and K. Jeong, "The Security Architecture for Secure Cloud Computing Environment," Journal of The Korea Society of Computer and Information, vol. 23, no. 12, pp. 81-87, 2018. doi:10.9708/jksci.2018.23.12.081
[20] Y. Cho and Y. Won, "A Methodology for Deriving an Information Security Framework for Network Services Based on ITU-T X.805," in Proceedings of the 24th Fall Conference of the Korea Information Processing Society, vol. 12, no. 2, pp. 1027-1030, 2005.
[21] B. Balakrishna, "Strategic Implementation of AWS Security Services: A Focus on Best Practices, SSM and Secrets Manager," Journal of Technology and Systems, vol. 6, no. 1, pp. 25-35, 2024. doi:10.47941/jts.1659
[22] V. Kasibhatla, "Navigating PCI DSS Compliance in the AWS Cloud," ISACA Journal, vol. 3, pp. 1-8, 2024.
[23] H. Yoo, K. Kim, and H.-J. Lee, "Research on automated inspection of electronic financial infrastructure vulnerabilities—focusing on security equipment," Journal of Korea Multimedia Society, vol. 29, no. 2, pp. 319-328, 2026. doi:10.9717/kmms.2026.29.2.319
[24] H.-W. Lee, "A Study on Cloud Security Architecture Complying with the Korean Electronic Financial Supervisory Regulations," Master's thesis, Graduate School of Information and Communications, Konkuk University, Seoul, Korea, 2023.
[25] J.-K. Lee, D. Min, and H.-Y. Kwon, "Issues and Suggestions for 'Act on the Development of Cloud Computing' and Protection of Its Users," Journal of Information Technology Applications & Management, vol. 24, no. 1, pp. 81-91, 2017. doi:10.21219/jitam.2017.24.1.081
[26] J. Woo, C. Kim, and H. Lee. "Research on the application of ISO 42001 for information security management in AI environments," The Society of Convergence Knowledge Transactions, vol. 13, no. 1, pp. 65-74, 2025. doi:10.22716/sckt.2025.13.1.006

Authors

Gyeongsu Kim received his M.S. degree in Digital Management from Korea University, Korea, in 2026. He is currently a Director at an information security consulting firm. He has over 20 years of professional experience in the information security field, including development, engineering, and security consulting. His main research interests include information security, cloud computing, privacy protection, and security architecture.

Hyunsu Yoo received his M.S. degree in Digital Management from Korea University, Korea, in 2026. He is currently the CEO of OpenSecureLabBiz, an information security consulting firm. He has over 21 years of professional experience in the information security field, including dev-ops. engineering. His main research interests include information security, and cloud computing.

Hanjin Lee received the B.S. in Sociology, M.S. degree in Communication from Yonsei University, Korea in 2006 and 2011. Furthermore he received the Ph.D. degrees in Digital Management, Korea University, 2021. His research interests are focused on AI biz innovation, user behavior and digitalization. He has gained 16 years experience in the Naver, eBay, and Coupang Corp.