다양한 산업에서의 키 관리 시스템 비교 분석

[1] 권우주, [2*]장항배

Comparison of key management systems across different industries

[1]Woojoo Kwon, [2*]Hangbae Chang

요 약

디지털 환경이 복잡해지고 사이버 공격이 정교해지면서 데이터 보호에 대한 중요성이 부각되고 있다. 데이터 유출, 시스템 침입, 인증 우회와 같은 다양한 보안 위협이 증가하면서 안전한 키 관리가 대두되고 있다. 키 관리 시스템(Key Management System, KMS)은 암호 키 생명주기 절차 전체를 관리하며, 여러 산업에서 사용되고 있다. 공공, 금융을 포함하는 다양한 산업의 환경에 맞는 요구 사항을 고려한 키 관리 시스템이 필요한 상황이다.

본 논문은 대표적인 산업에서 사용하는 키 관리 시스템을 비교 분석하여, 산업별 키 관리 시스템의 특성을 도출하는 것이 목적이다. 연구 방법은 문헌 및 기술 문서 분석, 사례 분석으로 정보를 수집하여, 산업 분야별 비교 분석을 진행하였다.

본 논문의 결과는 산업 환경에 맞는 키 관리 시스템을 도입하거나 개발 시 실질적인 가이드를 제공할 수 있을 것이다. 한계점은 분석한 산업 분야가 부족하고, 실험적 검증이 부족하였다. 이에 향후 연구에서 다양한 분야의 키 관리 시스템을 포함하여, 실험을 통한 구체적인 성능 테스트를 진행하고자 한다.

Abstract

As the digital environment becomes more complex and cyber attacks become more sophisticated, the importance of data protection is emerging. As various security threats such as data leakage, system intrusion, and authentication bypass increase, secure key management is emerging. Key Management System (KMS) manages the entire encryption key life cycle procedure and is used in various industries. There is a need for a key management system that considers requirements suitable for the environment of various industries including public and finance.

The purpose of this paper is to derive the characteristics of the key management system for each industry by comparing and analyzing key management systems used in representative industries. As for the research method, information was collected through literature and technical document analysis and case analysis, and comparative analysis was conducted by industry sector.

The results of this paper will be able to provide a practical guide when introducing or developing a key management system suitable for the industrial environment. The limitations are that the analyzed industrial field was insufficient and experimental verification was insufficient. Therefore, in future studies, we intend to conduct specific performance tests through experiments, including key management systems in various fields.

Keywords: *KMS, HSM , PKI, SSL, KDC*

[1] *중앙대학교 융합보안학과 석사과정 (tnswo2425@cau.ac.kr)*
[2*] *교신저자 중앙대학교 산업보안학과 교수 (hbchang@cau.ac.kr)*

Received: Jun. 03, 2024, Revised: Jun. 11, 2024, Accepted: Jun. 25, 2024

I. 서론

디지털 보안 환경의 복잡성과 사이버 공격이 증가함에 따라서 정보 보호의 중요성이 나날이 부각되고 있다. 데이터 유출, 시스템 침해, 인증 우회 등과 같이 보안 위협이 다양해지면서, 안전하고 효율적인 키 관리의 필요성이 증가하고 있다. 이때, 키의 생성, 저장, 배포, 갱신, 파기 등의 전반적인 키 관리 절차에서 키를 안전하고, 효율적으로 관리할 수 있게 해주는 것이 바로 키 관리 시스템이다[1].

금융, 공공, 클라우드 서비스, 제조 및 산업 등과 같이 다양한 산업에서는 각기 다른 운영 환경으로 인해 보안 요구 사항이 상이하기 때문에, 산업 분야별 맞춤형 키 관리 시스템을 필요로 한다. 이러한 경우 각 산업 분야에서 사용되는 키 관리 시스템의 특징과 성능을 비교 분석하여, 보안 요구 사항에 맞는 맞춤형 키 관리 시스템을 도출하여, 키 관리 시스템 선택 시 참고할 수 있는 연구가 필요하다.

본 논문의 목적은 대표적인 산업 분야인, 공공, 금융, 클라우드 서비스, 제조 및 산업 분야에서 사용되는 키 관리 시스템의 각 특징과 성능을 분석하고, 비교하여, 각 분야에 최적화된 키 관리 시스템의 특징과 성능을 도출하여, 키 관리 시스템을 선택하는 데 있어, 가이드라인을 제공하는 것이 목적이다.

II. 연구방법

본 연구의 키 관리 시스템 분석을 위해 다음과 같은 기준을 적용하여 선정하였다. 첫째는 연구에 포함될 시스템은 공공, 금융, 클라우드 서비스, 제조 및 산업 분야에서 널리 사용되고 있는 키 관리 시스템이어야 하고, 둘째는 보안성, 효율성, 관리 용이성을 포함한 주요 성능 지표에 대한 정보가 제공되는 시스템을 선택하였으며, 셋째는 산업 표준을 준수하거나 최신 기술을 사용하는 등 산업 분야별 보안 요구 사항에 맞는 시스템인지 고려하였다.

해당 선정 기준을 기반으로 각 산업 분야별로 보안 요구 사항과 기능을 충족하는 키 관리 시스템을 선정하고, 각 산업 분야별 성능과 적합성을 비교 분석하고자 한다.

III. 키 관리 시스템 비교

3.1 키 관리 시스템 구조 및 특징

키 관리 시스템의 구조는 크게 서버, 하드웨어 보안 모듈(Hardware Security Module, HSM), 데이터베이스, 클라이언트로 구성된다. 서버는 키 생성, 배포, 저장, 갱신, 파기 등 키의 전반적인 생명주기를 관리하며, 하드웨어 보안 모듈 및 데이터베이스와 통합된다. 하드웨어 보안 모듈은 생성된 키에 대해 안전하게 저장하고, 관리하며, 암호화, 해싱, 디지털 서명 등을 수행할 수 있다. 클라이언트는 사용자가 키 관리 시스템 서버를 생성하고, 관리할 수 있는 그래픽 사용자 인터페이스를 제공한다[2].

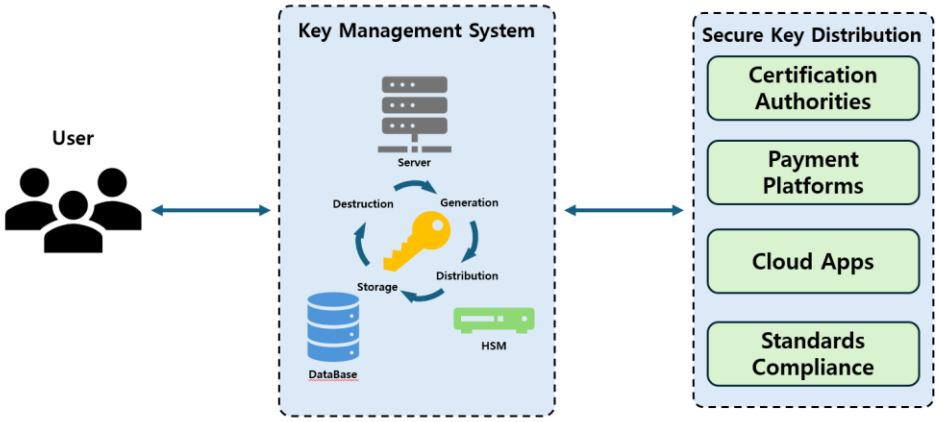

Figure 1. Architecture of KMS with functions and applications[2]
그림 1. 응용 프로그램과 기능이 포함된 키 관리 시스템 구조[2]

키 관리 시스템은 암호 키의 생성부터 폐기까지의 전체 과정을 안전하고 효율적으로 관리하기 위한 시스템으로, 다양한 구성 요소와 기능을 포함한다. 예를 들어, 키 생성 모듈은 예측 불가능한 난수를 생성하는 난수 생성기를 활용하여, 키를 생성하고, 키 저장은 물리적 또는 논리적으로 안전한 장치에 저장된다[3].

또한, 키 관리 시스템은 크게 키 배포 모듈, 키 갱신 및 폐기 모듈, 키 모니터링 모듈로 내부가 구성되어 있다. 키 배포 모듈은 인가된 사용자 또는 시스템에 키를 안전하게 배포하기 위해, 암호화된 통신 채널을 사용하며, 키의 기밀성과 무결성을 보장하기 위해, 키 전송 프로토콜을 사용하여 키를 전송한다. 키 갱신 및 폐기 모듈은 필요에 따른 키 갱신이 가능하며, 더 이상 사용하지 않는 키를 폐기하여, 키의 유출이나 재활용을 방지한다. 키 모니터링 모듈은 키의 생성, 배포, 저장, 갱신, 폐기 과정을 실시간으로 모니터링하여, 공격를 탐지할 수 있으며, 관리자에게 친근한 인터페이스를 제공하여 편의성을 제공해주기도 한다[3].

키 관리 시스템의 전체적인 구조와 내부 구성 요소들로 암호 키의 전체 생명주기를 관리하며, 보안성, 효율성, 관리 용이성 등의 측면에서 키 관리의 요구 사항을 만족시킬 수 있다.

또한, 키 관리 시스템은 중요 데이터를 보호하기 위해 적절한 접근 제어 시스템을 포함해야 하며, 인증된 사용자만 키 및 데이터 관리 기능을 수행할 수 있도록 보장하여, 암호 모듈과 연계하여 키의 무결성과 기밀성을 유지할 수 있다[4].

3.2 산업 분야별 키 관리 시스템 분석

공공 분야에서의 키 관리 시스템은 공공 환경에서 규제에 맞춰, 안전한 데이터 사용을 제공하고 있으며, 키 생명주기 절차는 키 생성, 설정, 키 입력 및 출력 그리고 저장, 삭제로 구성되어 안전하게 키를 관리한다. 키 생성 시 난수 생성기를 활용하고, 키 설정은 전자서명 인증체계 기반으로 공인된 암호 알고리즘을 사용한다. 암호 모듈로부터 키가 입출력되며, 전자서명인증체계의 암호 알고리즘을 이용해 암호화된다. 저장 시에는 평문 또는 암호화된 형식으로 저장되고, 사용이 끝난 키는 재활용 및 유출 방지를 위해 삭제한다. 이에 사용자는 안전하게 서비스를 이용할 수 있다[5].

추가적으로, 공공 분야의 키 관리 시스템은 대규모 인프라를 대상으로 하기에 키 관리 절차의 자동화와 중앙 집중형 관리를 통해 운영 효율성을 높인다. 특히, 정부기관은 다양한 법적 규제와 정책을 준수해야 하므로, 높은 수준의 감사 추적 기능과 규정 준수 보고 기능을 포함하고 있어야 한다.

금융 분야에서의 키 관리 시스템은 안전한 금융 거래를 위해 설계되었고, 주로 공개키 기반 구조(Public-Key Infrastructure, PKI)이다. 국제적으로 통용되는 TLS/SSL 프로토콜을 금융기관의 요구 사항에 맞게 변형시켜 사용하고 있다. 키 생명주기 절차는 키 생성, 분배, 저장, 사용, 백업 및 복구, 교체, 폐기로 보안성 있는 관리를 하고 있다. 키 생성 시 난수 생성기를 활용하고, 키

분배센터(Key Distribution Center, KDC)를 이용하여 키를 분배한다. 여기서 키 분배센터는 모든 사용자가 완전히 신뢰하여, 제 3자 입장에서 키를 분배해주는 역할을 한다. 키 저장은 암호 모듈을 사용하고, 접근 제어 정책을 수립한 후 키를 사용한다. 이후 키 백업 및 복구 정책이 수립되며, 키 용도에 따라 내부 정책에 맞는 키 교체가 이루어지며, 사용하지 않는 키는 재활용 및 유출 방지를 위해 폐기 처리한다. 또한, 다양한 사이버 공격에 취약할 수 있어 다층 보안 메커니즘과 실시간 모니터링 시스템을 필요로 하는데, 이는 위협적인 활동을 신속하게 탐지하고 대응할 수 있으며, 금융 거래의 연속성과 무결성을 유지할 수 있다. 금융 데이터는 민감성이 높아 강력한 데이터 암호화와 키 관리 정책이 요구된다.

추가적으로, 금융기관은 키의 안전성을 보다 강화하기 위해, FIPS 140-2 수준의 보안 등급을 준수하는 암호 모듈을 사용하게 된다. 키 생성 시에는 SSL, TLS, IPSec 등의 공개키 알고리즘을 사용해 자동화된 방법과 수동 전달 방식을 조합하여 사용하며, 키의 입력 및 출력은 인가된 관리자가 직접 수행하고, 스마트카드나 토큰을 이용한 전자적인 방법을 주로 사용한다[6].

클라우드 서비스 분야에서의 키 관리 시스템은 클라우드 환경에서 데이터의 기밀성을 위해 설계되었으며, 암호 키 생성, 저장, 관리 및 계층적 키 관리 방식을 이용한 안전한 키 관리 방식을 제공하게 된다. 해당 키 관리 시스템은 데이터 키, 마스터 키, 루트 키 등의 계층적인 암호화 방식을 사용하며, 생성된 마스터 키는 하드웨어 보안 모듈에 저장하는데, FIPS 140-2 레벨 3 표준을 준수하여, 안전성을 강화하였다. 또한, 자동 키 로테이션, 키 정책 설정, 감사 로그 제공 등 다양한 기능을 통해서 보안성을 강화할 수 있다. 이에, 사용자는 각 서비스에서 데이터를 안전하게 사용할 수 있다[7].

추가적으로, 데이터의 분산 저장 및 멀티 테넌트 환경으로 인해 보안 관리가 복잡해질 수 있어, 클라우드 제공자는 다층 보안 체계와 데이터 격리 기술을 적용하여, 테넌트 간의 데이터 접근을 철저히 통제한다. 또한, 클라우드 환경의 특성상 동적 스케일링이 가능해야 하므로, 키 관리 시스템도 이에 맞춰 유연하게 확장될 수 있어야 한다.

제조 및 산업분야에서의 키 관리 시스템은 제조 및 산업 환경에서 데이터의 기밀성, 무결성, 가용성을 보장하고 있으며, 키 생명주기 절차를 효율적으로 관리한다. FIPS PUB 186-2 및 PKCS#11 인터페이스 표준을 준수하고, 하드웨어 보안 모듈을 적용한 안전한 키 관리가 이루어진다. 관리자 중심의 편리한 시스템을 제공하기 위해 모니터링과 스케줄링 기능을 지원하고 있다. 이에 제조 및 산업부문 기업들은 효율적이고 안전한 운영을 할 수 있다[8].

추가적으로, 사이버-물리 시스템(Cyber Physical System, CPS)과 사물인터넷(Internet Of Things, IoT) 등의 기술 도입으로 인해 복잡한 보안 요구 사항이 발생한다. 특히, 실시간 데이터 처리와 무결성 보장이 중요한 제조 환경에서는 엄격한 키 관리와 빠른 키 갱신이 필수적인 요소이며, 이를 통해 생산 연속성을 유지하고, 잠재적인 보안 위협을 신속히 차단할 수 있다.

3.3 분석 결과 및 비교

적합한 키 관리 시스템을 선택할 때, 고려하는 요구 사항을 기반으로 분석 항목을 선정한다. 분석 항목은 보안 수준, 사용성 및 관리 편의성, 성능 그리고 비용으로 각 산업 분야별로 분석하고자 한다. 그리고 분석하기에 앞서, 각 분석 항목에서 무엇을 고려할지 파악하기 위한 설명을 진행하고자 한다.

첫 번째 항목은 보안 수준으로 데이터의 기밀성, 무결성, 가용성을 보장하는 수준과 외부 공격 및 내부 위협으로부터 대응하는 수준을 나타내는 항목이다. 두 번째 항목은 사용성 및 관리 편의성으로 키 관리 시스템을 사용하는 데에 있어, 키 사용에 대한 접근 통제나 시스템의 직관적인 인터페이스와 자동화 기능을 통해 시스템을 쉽게 사용할 수 있는 정도를 말하며, 이는 키 관리 시스템의 효율성을 높이는 데 필수적이다. 세 번째 항목은 성능으로 키 생명주기 절차에 따른 처리 속도와 시스템 자원 사용률을 말하며, 대규모 데이터 처리가 필요한 환경에서 효율적으로 동작할 수 있는지 확인할 수 있으며, 키 관리 시스템의 효율성을 확인하는 데 필요한 항목이다. 네 번째 항목은 비용으로 키 관리 시스템의 초기 도입부터 운영까지의 사용되는 전체적인 비용을 확인하는 항목이며, 각 산업 분야는 사용 가능한 비용에 대한 제약이 있기 때문에, 정해진 예산 안에서 요구 사항을 충족시키기 위해 필요한 항목이다.

각 항목을 분석하여, 각 산업 분야의 요구 사항에 맞는 키 관리 시스템을 선택할 수 있을

것이다. 다음으로 각 분석 항목을 각 산업 분야별로 분석하고자 한다.

첫 번째로 보안 수준을 분석하였을 때, 공공 분야는 대국민 사용에 의한 데이터 보안을 위해 전자서명법을 준수한다. 금융 분야는 안전한 금융 거래를 위해 FIPS 140-2 표준과 맞춤형 보안 프로토콜을 사용한다. 클라우드 서비스 분야는 데이터 사용의 신뢰성을 위해 하드웨어 보안 모듈을 사용하여 키를 저장한다. 제조 및 산업 분야는 데이터 보안성을 위해 FIPS PUB 186-2 및 PKCS#11 인터페이스 표준과 하드웨어 보안 모듈을 사용한다.

두 번째로 사용성 및 관리 편의성을 분석하였을 때, 공공 분야는 접근 제어 정책으로 허가된 관리자가 키를 관리하고, 실시간 모니터링도 가능하다. 금융 분야는 승인된 암호기술을 사용하고, 관리자가 직접 키를 관리한다. 클라우드 서비스 분야는 사용하기 편리한 인터페이스를 제공하고, 자동으로 키를 관리한다. 제조 및 산업 분야는 클라우드와 온프레미스 환경에서 운영이 가능하다는 장점이 있고, 모니터링 및 자동 키 관리 기능이 있다.

세 번째로 성능을 분석하였을 때, 공공 분야는 전자서명 관련 작업을 효율적으로 수행한다. 금융 분야는 키 관리 절차가 복잡하지만, 고속 난수 생성기와 고성능 암호 모듈을 사용하여, 처리 속도가 빠르다. 클라우드 서비스 분야는 계층적 키 관리 방식을 사용하여, 키 관리 절차가 효율적이고, 대규모 환경에서 적용 가능하다. 제조 및 산업 분야는 고성능 암호 모듈을 사용하여, 처리 속도가 빠르다.

네 번째로 비용을 분석하였을 때, 공공 분야는 국가 인프라 보안을 위한 규정과 보안에 비용이 많이 사용된다. 금융 분야는 안전한 금융 거래를 위해 초기 도입 비용과 유지보수에 많은 비용이 사용된다. 클라우드 서비스 분야는 사용량에 따라 비용을 지불하므로, 초기 도입 비용이 낮은 편이다. 제조 및 산업 분야는 자동화된 키 관리로 운영에서 비용을 절감할 수 있다.

키 관리 시스템을 도입 및 개발할 때는 해당 분야에 맞는 특성과 요구 사항을 고려해야 한다. 예를 들어, 금융 분야에서는 높은 보안성과 빠른 처리 속도를 요구한다. 보안성을 위해 키 관리 절차가 복잡해져 처리 속도가 늦어지게 된다. 이때, 처리 속도를 올리기 위해 고성능 모듈을 사용한다. 그러나 고성능 모듈은 비용이 많이 들게 된다. 이처럼 분야별 특성과 요구 사항에 따라 보안성과 효율성을 균형 있게 맞춰 키 관리 시스템을 도입하거나 개발하는 것이 중요하다.

Table 1. Compare Key Management Systems by Field
표 1. 분야별 키 관리 시스템 비교

Criteria	Public Sector	Financial Sector	Cloud Service	Manufacturing & Industrial
Security Level	Compliance with e-Signature Law, High Security	Compliance with FIPS 140-2, SSL/TLS	HSM, Automatic Key Rotatio	Centralized Management, Real-time Monitoring
Usability & Management Ease	Strict Access Control, Real-time Monitoring	Supports Various Encryption Algorithms	User-friendly Interface	Supports Cloud & On-premises, Automation
Performance	Optimized for Large-scale Data Processing	High-speed RNG, Efficient Encryption	Hierarchical Key Management	High-speed Encryption Module, Performance Optimization
Cost	High Security Maintenance Costs	Initial Setup & Maintenance Costs	Usage-based Pricing Model	Reduced Operating Costs, High Applicability

IV. 시사점

본 연구는 산업 분야별 키 관리 시스템을 비교 분석하여, 시스템 환경에 맞는 키 관리 시스템 도입 및 개발의 중요성을 파악하였다. 이를 통해 맞춤형 키 관리 시스템 도입 및 개발에 가이드라인을 제공하고자 한다. 본 연구의 학술적 및 산업적 관점에서의 시사점은 다음과 같다.

먼저, 학술적 관점에서는 본 연구에서 확인한 산업 환경에 맞는 키 관리 시스템의 필요성으로,

맞춤형 키 관리 시스템 개발에 대한 연구의 방향성을 제시하여, 다양한 산업 분야에서 요구되는 보안 요구사항을 충족시키기 위해서는 맞춤형 키 관리 시스템의 설계 및 구현에 대한 심도 있는 연구가 필요함을 시사한다.

산업적 관점에서는 산업 분야별 특성과 요구 사항을 고려한 키 관리 시스템의 도입이나 개발 시 보안성과 효율성의 균형이 잘 맞춰진 시스템을 구축할 때 도움이 될 수 있다. 특히, 공공, 금융, 클라우드 서비스, 제조 및 산업 분야 등 각 산업의 고유한 요구 사항을 충족시키기 위해 적합한 키 관리 시스템을 도입하거나 개발하는 과정에서 실질적인 가이드라인을 제공할 수 있을 것이다.

V. 결론

본 연구는 각 산업 분야에서 사용되는 대표 키 관리 시스템 선정하고, 비교 분석하여, 각 분야에 최적화된 특징과 성능을 분석하였다. 이를 통해 각 산업 분야의 특성과 요구 사항을 충족하는 키 관리 시스템을 선택하는 데에 실질적인 지침을 제공함으로써, 키 관리 시스템의 발전에 기여할 것이라 생각한다.

한계점으로는 주요 산업 분야의 대표적인 키 관리 시스템을 중심으로 비교 분석하였으며, 그 외의 키 관리 시스템을 포함하지는 못하였다. 또한, 실험적 검증이 부족하여 키 관리 시스템의 실제 성능을 정확하게 평가하지 못한 한계가 있다. 향후 연구에서는 더 다양한 키 관리 시스템을 포함하고, 실제 환경에서의 실험을 통한, 구체적인 성능 테스트를 할 필요가 있다.

VI. 감사의 글

이 논문은 2024년도 중앙대학교 연구 장학기금 지원에 의한 것임.

VII. 참고문헌

[1] J. Y. Lee, “[KAIST Graduate School of Information Security Relay Column-2] Security Limits and Standardization Trends of Block Cipher Operation Modes,” BoanNews, 2024. [Online]. Available: https://m.boannews.com/html/detail.html?tab_type=1&idx=128376

[2] Levgeniia Kuzminykh, Bogdan Ghita, Stavros Shiaeles, "Comparative Analysis of Cryptographic Key Management Systems", Lecture Notes in Computer Science, vol. 12526, pp. 80–94, Dec. 2020.

[3] Elaine Barker, Miles Smid, Dennis Branstad, Santosh Chokhani, "A Framework for Designing Cryptographic Key Management Systems," National Institute of Standards and Technology, NIST Special Publication 800-130, Aug. 2013.

[4] Shahnawaz Ahmad, Shabana Mehfuz, Javed Beg, "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment", The Journal of Supercomputing, vol. 79, pp. 7377–7413, 2023.

[5] Korea Internet & Security Agency, "Technical Specification for Electronic Signature Key Protection v1.11," Sept. 2009.

[6] Y. K. Kim, “Guide to the Use of Cryptographic Technologies in the Financial Sector,” Financial Security Institute, Jan. 2019.

[7] Amazon Web Service, "AWS Key Management Service," Amazon Web Service, 2024.

[8] AUTOCRYPT, "AutoCrypt Key," AUTOCRYPT, 2024. [Online]. Available: https://autocrypt.co.kr/autocrypt-key/

저자소개

권우주 (*Woojoo Kwon*)

2014 년~2020 년 신라대학교 컴퓨터공학과(학사)
2022 년~현재 중앙대학교 융합보안학과 산업보안기술전공(석사과정)

관심분야 : 산업보안, 정보보안, 블록체인, 컴퓨터시스템

장항배 (*Hangbae Chang*)

2007 년~2012 년 대진대학교 경영학과 조교수
2012 년~2013 년 상명대학교 경영학과 조교수
2014 년~현재 중앙대학교 산업보안학과 교수

관심분야 : 산업보안, 정보등급화, 보안데이터분석, 연구보안, 클라우드 보안