사물인터넷융복합논문지 Vol. 10, No. 4, pp. 65-70, 2024 https://doi.org/10.20465/KIOTS.2024.10.4.065

사물인터넷 환경에서 보안 액세스 서비스 에지 교육과정 모델에 관한 연구

이근호*
백석대학교 컴퓨터공학부 교수

A Study on Curriculum Model for Secure Access Service Edge in IoT Environment

Keun-Ho Lee*
Professor, Div. of Computer Engineering, BaekSeok University

요 약 사물인터넷 환경에서 새로운 보안에 대한 요구사항은 빠르게 변화하고 있다. 이러한 빠른 변화에서 보안 위협을 통한 침해사고가 발생하면 큰 피해가 발생한다. SASE(Secure Access Service Edge) 환경은 보안 위협에 매우 취약하며, 침해가 발생하면 심각한 피해가 발생한다. SASE 환경의 보안을 강화하려면 SASE의 고유한 특성과 문제 해결을 다루는 전문 커리큘럼이 필요하다. 본 논문에서는 SASE 환경 내에서 보안 사고에 대응하기 위한 커리큘럼 모델을 제안한다. 제안된 커리큘럼 모델은 위협 유형, 위반 시나리오 및 대응 절차를 포함하여 SASE 보안의 다양한 측면을 다루는 교육과정으로 설계하였다. 이 모델의 목표는 보안 인식을 향상하고 전문가가 SASE 프레임워크 내에서 보안 사고를 효과적으로 처리할 수 있도록 준비하는 것에 목적을 두고 있다.

주제어 : 사물인터넷, 보안 액세스, 서비스 에지, 정보보호, 교육과정, 보안 위협

Abstract In the Internet of Things environment, new security requirements are changing rapidly. In this rapid change, if a breach occurs due to a security threat, great damage will occur. The SASE (Secure Access Service Edge) environment is highly vulnerable to security threats, and if a breach occurs, serious damage will occur. In order to strengthen the security of the SASE environment, a specialized curriculum that covers the unique characteristics and problem solving of SASE is required. In this paper, we propose a curriculum model for responding to security incidents in the SASE environment. The proposed curriculum model is designed to cover various aspects of SASE security, including threat types, breach scenarios, and response procedures. The goal of this model is to increase security awareness and prepare professionals to effectively handle security incidents within a SASE framework.

Key Words : IoT, Secure Access, Service Edge Information Security, Curriculum, Security threat

1. 서론

사물인터넷(IoT)은 사물과 사물 간의 통신을 통해 정보를 교환하고 제어하는 기술로 다양한 네트워크 환경에서 운영이 된다. 이러한 운영에서 필요한 부분은 안전한 네트워크 환경에 대한 보안설계가 중요하다. 최근 다양한 공격그룹은 공격 대상 기업의 임직원 단말을 거점으로 활용, 외부에 노출된 계정 활용, 유통망을 이용한 공격 등으로 글로벌 보안 기술을 선도하는 기업의 보안망을 무력화하고 공격에 성공하고 있다. 기업은 현재 보안

이 논문은 2024학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2024년 07월 12일 수정일 2024년 08월 04일 심사완료일 2024년 08월 14일

수준으로 안전하다는 관념을 버리고 새로운 기술과 관리 체계의 도입 검토가 필요한 상황이다. 2021년 8월 Cisco, 2022년 9월 Uber 그리고 2023년 Microsoft까지 글로벌한 해킹조직에 의해 IT 선도 기업들이 해킹 사고로 인한 피해가 발생하였다. 특히 IT 보안 솔루션과 서비스를 공급하는 Cisco와 Microsoft사의 피해는 글로벌한 공격 조직의 능력을 가늠할 수 있게 되었다. 이제 네트워크로 연결된 세상에 어떠한 기업도 고도화된 공격그룹으로부터 완벽하게 공격을 방어할 수 없다는 것을 증명하고 있다. 이러한 보안 공격의 시대적 변화에 따라 제로트러스트에 대한 관심이 높아지고 있다. 제로 트러스트는 위치, 사용 이력과 관계없이 네트워크 및 자원에 접근하는 모든 사용자를 인증한 후 최소 접근 권한만 제공하는 보안 모델이다. 제로트러스트는 원칙과 원리를 제공하고 있다. 이러한 원칙과 원리를 기술적 요소, 관리적 요소를 포함하여 기업 인프라에 적용한 구체적 아키텍처와 모델이 제로트러스 아키텍처(ZTA: Zero Trust Architecture)이다. 제로트러스트 아키텍처의 구현 모델로는 ZTNA, ZTE, ZT Security 등이 존재하며 향후 더 많은 모델이 발표될 수 있다[1-5]. IoT는 다양한 산업 분야에서 활용되고 있으며, 그 규모는 빠르게 증가하고 있다. SASE (Secure Access Service Edge)는 클라우드 기반의 네트워크 아키텍처 모델로, 보안과 네트워크 기능을 통합하여 제공하는 접근 방식이다. SASE는 기업이 클라우드 환경에서 효율적으로 작업할 수 있도록 설계되었으며, 네트워크와 보안을 함께 관리할 수 있는 통합 솔루션을 제공한다[6].

본 연구에서는 보안 엑세스 서비스 에지 관련 연구를 통하여 기존에 제안하고 있는 사물인터넷 환경에서의 제로트러스트 관련 기술에 대한 내용을 살펴보고, 제안한 교육 내용에서 좀 더 기업체의 맞춤형 교육과정에 대한 모델을 제안하고자 한다. FGI(Focus Group Interview)를 통한 제로트러스터 분야의 선두기업 2개사의 주요 요구사항을 접목한 교육과정 모델을 설계하고자 한다. 본 교육과정 모델을 위하여 기존에 진행했던 침해사고대응 기반의 인재양성 사업의 교육과정 개발과 적용 경험을 바탕으로 제로트러스트 기반 보안 엑세스 서비스 에지 운영의 모델을 제안하고자 한다.

2. 관련 연구

2.1 사물인터넷 침해사고 교육 모델

IoT 환경에서의 침해사고대응은 매우 중요하다. 침해사고가 발생하면 IoT 환경에 큰 피해를 주고, 침해사고로 인해 IoT 장비가 제어를 잃거나 IoT 장비에 저장된 개인 정보가 유출될 수 있다. IoT 환경에서의 침해사고 대응 절차는 침해사고를 탐지, 침해사고의 원인을 조사, 침해사고의 영향을 평가, 침해사고 복구, 침해사고를 예방하기 위한 조치를 취한다. IoT 환경에서의 침해사고를 예방하기 위해서는 IoT 장비를 안전하게 설정하고, IoT 장비를 최신 상태로 유지하며, IoT 장비에 대한 보안 패치를 설치하고, IoT 장비에 대한 보안 인식을 높이기 위한 교육 등의 다양한 관리체계에 대한 조치를 취해야 한다[7-12].

2.2 제로트러스트

제로트러스트 아키텍처는 기업의 환경 수준에 따라 구현 레벨에 차이가 있고, 변화하는 위협에 따라 지속적으로 적응하고 발전시키는 고도화 작업이 반복되어야 한다. 이에 제로트러스트 아키텍처의 성숙도 모델을 통해 기업의 현 단계를 평가하고 최적화 단계로 진입하기 위한 활동과 적용 계획을 수립해야 한다. ZTA(Zero Trust Architecture)는 보고서에서는 변화하는 인프라 환경을 보호하기 위해 과거의 경계보안모델의 한계를 극복을 위해 “제로 트러스트 모델”이라는 중요구성요소의 기술적, 관리적 보호조치 개선하는 자세한 내용이 포함되어 있다. 2023년 9월 NIST는 800-207A를 발표하여 멀티 클라우드 및 하이브리드 환경에 대한 ZTA의 런타임 요구사항을 충족하고, 세분화된 애플리케이션 통제 아키텍처를 구축하기 위한 가이드가 추가로 개정되었다. 이와 같이 ZTA는 ZTMM(Zero Trust Maturity Model)을 기반으로 한 성숙모델과 환경에 변화에 따라 지속적으로 발전해가는 개념적 모델이다[1-6].

다음은 제로트러스터 접속방법에 따른 보안통제에 대한 분석 내용이다[7].

- 외부에서 내부로 접속시

외부의 접속을 시도하는 모든 행위 주체는 대해 인증을 위한 아이덴티티 서비스 또는 API 접속 인증을 거쳐 위치에 가장 가까운 클라우드 POP을 거쳐 보안 정책을 반영받고, 클라우드 POP을 통해 Firewall, SWG(Secure Web Gateway), IPS, NGAM(Next-Generation Anti-Malware)의 보안검증을 수행하고 허가된 접속 대역 및 서비스로만 경로가 허가되고, 내부 기밀 리소스 접근 시, 접근통제 체계를 통해 권한에 부여된 자산에 접속이 가능하도

록 구성한다.

- 외부에서 외부로 접속

외부에서 외부로 접속하는 것에 대해 일반 인터넷은 서비스 연결을 위한 별도의 아이덴티티 검증을 수행하지 않으며, 추가적으로 외부에 있는 행위주체로 인해 리스크 사이트 접속 및 주요정보 유통을 통제하기 위해 NGFW(Next-Generation Firewall), SWG, DLP(Data Loss Prevention) 기능을 적용해야 하고, 외부에 존재하는 행위주체로 위협요소가 유입되는 것을 차단하기 위해 NGAM을 적용해야 하여, 사용자가 업무 용도로 접속하지만 안전성 평가가 되지 않은 잠재적 위협 사이트 접속을 위해서는 웹격리 기능을 통해 악성 컨텐츠 유입을 원천적으로 차단한다.

- 내부에서 외부로 접속

내부에서 외부로 접속하는 것에 대해 일반 인터넷은 서비스 연결을 위한 별도의 아이덴티티 검증을 수행하지 않고, 추가적으로 외부에 있는 행위주체로 인해 리스크 사이트 접속 및 주요정보 유통을 통제하기 위해 NGFW, SWG, DLP 기능을 적용해야 하고, 외부에 존재하는 행위주체로 위협요소가 유입되는 것을 차단하기 위해 Virus Wall을 적용하여, 사용자가 업무 용도로 접속하지만 안전성 평가가 되지 않은 잠재적 위협 사이트 접속을 위해서는 웹격리 기능을 통해 악성 컨텐츠 유입을 원천적으로 차단한다.

2.3 SASE(Secure Access Service Edge)

SASE는 기존 네트워크 경계 내부와 외부의 네트워크 요소를 보호하는 제로 트러스트 아키텍처의 구성 요소이다. 비즈니스의 디지털 혁신, 증가한 원격 작업, 그리고 애플리케이션을 실행하기 위한 클라우드 서비스 이용과 더불어 보안이 클라우드로 이동하고 있으며 SASE는 그러한 보안을 제공하고 있다. SASE의 주요 요소는 다음과 같다[6].

- 클라우드 기반의 네트워크: SASE는 클라우드 네트워크를 기반으로 하여, 모든 사용자가 네트워크에 안전하게 접근할 수 있도록 한다. 이는 중앙 집중식 관리와 스케일러빌리티를 제공하며, 다양한 지역과 지사에서 동일한 보안 및 네트워크 정책을 적용할 수 있게 한다.
- 통합 관리: SASE는 네트워크와 보안 기능을 통합하여 단일 플랫폼에서 관리할 수 있도록 하고, 이는 IT 관리의 복잡성을 줄이고, 일관된 정책 적용을 가능하게 한다.
- 사용자 및 디바이스 중심의 접근: SASE는 사용자가 어디서든지 안전하게 네트워크에 접근할 수 있도록 지원하며, 클라우드 애플리케이션이나 서비스를 사용해도 보안이 유지되도록 한다.
- 유연성과 확장성: 클라우드 기반으로 설계된 SASE는 필요에 따라 쉽게 확장할 수 있으며, 글로벌 지사나 원격 근무자들에게도 적절한 성능과 보안을 제공한다.
- 보안 기능 통합: SASE는 여러 보안 기능을 통합하여 제공하며 다음과 같다.
  · SD-WAN: 소프트웨어 정의 WAN은 네트워크 트래픽을 관리하고 최적화하여 성능을 향상시키는 기능을 제공
  · ZTNA(Zero Trust Network Access) : 네트워크 접근을 요구하는 사용자나 디바이스가 신뢰할 수 없는 것으로 간주하고, 그에 맞는 인증과 권한 부여를 수행
  · CASB(Cloud Access Security Broker) : 클라우드 애플리케이션의 사용을 모니터링하고 제어
  · 위협 방어: 네트워크를 통한 악성 소프트웨어나 공격으로부터 보호

결국 SASE는 현대의 분산된 업무 환경과 클라우드 기반 서비스의 증가에 대응하기 위해 설계된 모델로, 네트워크와 보안을 통합하여 보다 효율적이고 유연한 IT 인프라를 제공한다[1-6].

3. SASE 교육과정 모델 설계

3.1 Focus Group Interview

Focus Group Interview 을 통한 SASE 분야의 선두기업인 2개 사의 사업과 관련된 기술 수요를 확인하여 관련 분야 인재양성의 목적의식이 뚜렷한 A사, B사를 참여기업으로 선정하여 수요 내용을 확인하였다. 결과 내용으로는 SASE에 대한 기본 개념과 기술적 중요성을 이해하고, SASE 아키텍처, SD-WAN 기능과 구현, 네트워크 보안 기능, 원격 접속 및 모바일 사용자 보호, 데이터 보호 및 컴플라이언스, 성능 최적화 및 트래픽 관리, 모니터링 및 운영관리 등을 중점으로 교육의 필요성을 확

인하였다.

교육과정은 사물인터넷 환경의 변화에 맞추어 변경이 되고 있는 클라우드 기반의 특성을 고려하여 설계되어야 하고, 사물인터넷 환경은 기존의 IT 환경과는 다른 특성을 가지고 있어, 연결된 장치의 수가 많고, 장치의 성능이 낮으며, 보안 기능이 취약한 특성을 고려하여 교육과정은 사물인터넷 환경에서 발생할 수 있는 보안 사고의 유형과 대응 방법을 포함하도록 설계가 이루어져야 한다. 교육과정은 실습 위주로 진행되어야 하고, 실습 위주로 진행되는 교육과정은 학생들이 최근에 적용이 되고 있는 SASE관련 솔루션 기술을 실무적으로 적용하는 방법을 배울 수 있다. 교육과정은 최신 보안 기술 동향을 반영해야 하고, 보안 기술은 빠르게 변화하고 있어서 학생들이 최신 보안 기술을 배울 수 있도록 구성해야 한다.

세부적인 산업체 요구사항은 제로트러스트 기반 사고대응과 실무융합, 현장적응능력이 필요하다는 의견이었다. 2개사에서 제안한 교육과정 모델은 현재 실무에서 적용이 되고 있는 솔루션을 기반으로 하여 설계가 되었다.

3.2 SASE(Secure Access Service Edge) 교육 모델

[표1]에서 제안하고 있는 교육과정의 목표는 SASE의 기본 개념과 구성 요소(SD-WAN, 클라우드 기반 보안 서비스, 제로 트러스트 네트워크 접근)에 대한 이해, 네트워크 아키텍처 설계, 정책 설정, 보안 구성 등을 설계하고 구현하는 방법에 대한 이해, SASE 솔루션을 통해 네트워크 보안과 이해를 실습(실시간 위협 감지, 데이터 보호, 네트워크 트래픽 최적화 등의 기술), SASE 솔루션의 일상 운영 및 관리를 위한 실무 능력을 배양하고, 2개 참여기업에서는 직무역량을 크게는 네트워크 기반 사고대응 모델링, 침해사고 및 악성코드 분석, 실무융합으로 나뉘어 구성하였다. SASE 기본개념 및 중요성 이해는 SASE의 기본개념과 필요성을 이해하고, 개요를 파악, SASE의 정의, 구성요소, 전통적 네트워크와의 차이점, SASE 개요로 구성하고 있다. SASE 아키텍처는 SASE의 아키텍처와 구성 요소를 상세 이해와 SASE의 네트워크 아키텍처, 클라우드 기반 보안 서비스, 글로벌 사설 백본, 통합 관리 콘솔로 구성하고 있으며, SD-WAN 기능

〈Table 1〉 Infringement response training course model customized for industry

No	Lecture content	Method	Time
1	▸Understanding SASE Basic Concepts and Importance · Understand the basic concepts and necessity of SASE, and get an overview · Introduction to SASE definition, components, differences from traditional networks, and SASE overview	Theory	3/0
2	▸SASE Architecture · Detailed understanding of SASE architecture and components · SASE network architecture, cloud-based security services, global private backbone, unified management console	Theory	3/0
3	▸SD-WAN features and implementation · Learn how to understand and configure SD-WAN features · Basic concepts of SD-WAN, SD-WAN features, setup and management methods	Theory	3/0
4	▸Network Security Functions · Understand the network security functions of SASE and learn how to strengthen security through them · Firewall, Threat Prevention, Zero Trust Network Access (ZTNA), Intrusion Prevention System (IPS)	Theory/ Practice	2/4
5	▸Remote Access and Mobile User Protection] · Learn how to build a secure access environment for remote workers · Remote Access Solutions, Mobile User Protection, Client Installation and Configuration	Theory/ Practice	2/4
6	▸Data Protection and Compliance] · Understand how to meet data protection and compliance requirements · Data encryption, data loss prevention (DLP), log management and auditing, compliance requirements	Theory/ Practice	2/4
7	▸Performance Optimization and Traffic Management] · Learn how to optimize network performance and effectively manage traffic · Traffic engineering, QoS (Quality of Service) settings, bandwidth management, optimization techniques	Theory/ Practice	2/4
8	▸Monitoring and Operations Management] · Learn how to perform continuous monitoring and operations management of CATO SASE solutions. · Real-time monitoring, setting up alerts and notifications, troubleshooting and reporting, and using operations management tools.	Theory/ Practice	2/4
9	▸Practical Training and Case Studies] · Develop the ability to design and configure SASE solutions based on scenarios · Practice designing and implementing solutions and solving problems in various environments	Theory/ Practice	2/4

과 구현은 SD-WAN 기능을 이해하고 구성하는 방법을 학습, SD-WAN의 기본 개념, SD-WAN 기능, 설정 및 관리 방법으로 구성하였다. 네트워크 보안 기능은 SASE의 네트워크 보안 기능을 이해하고, 이를 통해 보안을 강화하는 방법을 학습하며, 방화벽, 위협 방지, 제로 트러스트 네트워크 접근(ZTNA), 침입 방지 시스템(IPS)으로 구성한다. 원격 접속 및 모바일 사용자 보호는 원격 근무자를 위한 안전한 접속 환경을 구축하는 방법을 학습하고, 원격 접속 솔루션, 모바일 사용자 보호, Client 설치 및 설정한다. 데이터 보호 및 컴플라이언스는 데이터 보호 및 컴플라이언스 요구사항을 충족하는 방법을 이해와 데이터 암호화, 데이터 유출 방지, 로그 관리 및 감사, 컴플라이언스 요구사항으로 구성한다. 성능 최적화 및 트래픽 관리는 네트워크 성능을 최적화하고 트래픽을 효과적으로 관리하는 방법을 학습하고, 트래픽 엔지니어링, 서비스 품질 설정, 대역폭 관리, 최적화 기술로 구성한다. 모니터링 및 운영 관리는 C사 SASE 솔루션의 지속적인 모니터링과 운영 관리를 수행하는 방법을 학습한다. 실시간 모니터링, 경고 및 알림 설정, 문제 해결 및 보고, 운영관리 도구 사용하도록 구성한다. 실습 및 케이스 스터디는 시나리오를 기반으로 SASE 솔루션을 설계하고 구성하는 능력 배양하고, 다양한 환경에서의 솔루션 설계 및 구현, 문제 해결 실습으로 구성한다.

4. 결론

사물인터넷 기술은 빠르게 발전하고 있으며, IoT 환경에서 발생하는 보안 사고의 위험도 증가하고 있다. 이러한 보안 사고를 예방하고 대응하기 위해서는 최신 보안 동향을 이해하고 그에 맞는 교육과정을 통한 모델 설계가 중요하다. 최근 제로트러스트에 대한 많은 관심과 배경을 통하여 SASE 관련 다양한 제품에 대한 적용을 위한 노력이 진행되고 있다. 본 연구에서는 IoT 환경에서 보안 엑세스 서비스 에지를 위한 교육과정 모델을 제안하였다. 제안된 교육과정 모델은 제로트러스트 환경의 특성을 고려하여 설계되었다. 본 연구에서는 IoT 환경에서 보안 엑세스 서비스 에지를 위한 교육과정 모델을 제안하였으나, 몇 가지 한계가 있다. 첫째, 제안된 교육과정 모델은 사물인터넷 환경의 특성을 고려하여 설계되었지만, 사물인터넷 환경에서의 다양한 환경을 모두 만족시킬수 없으며, 일반적인 시스템 환경을 기반으로 고려하여 설계가 되었다. 제안된 교육과정 모델은 실무에서 적용하고자 하는 서비스와 솔루션을 기반으로 하고 있지만 너무 빠르게 변화하고 있는 보안의 솔루션을 전부 적용하기에는 어려움이 있다. 셋째, 제안된 교육과정 모델은 실습 위주로 진행되기 위해서는 관련된 제품 솔루션의 구매가 선행이 되어야 하는데 이에 대한 솔루션 도입 및 구축이 학교 현장에 따라 어려움이 있을 수 있으면 제품도 국내외 제품의 종류에 따라 차별화된 교육의 체계가 좀 더 보완이 되어야 좀 더 좋은 교육과정으로 발전시켜 갈 수 있으므로 향후에는 각 제품별로 분석을 통한 내용으로 제안된 교육과정 모델의 교육 효과를 검증하고, 교육과정 모델을 지속적으로 업데이트해야 하고, 실습 환경을 구축하는 데 드는 비용을 줄일 수 있는 방안을 연구하고자 한다.

REFERENCES

[1] John Kindervag, “No More Chewy Centers: TheZero Trust Model Of Information Security,”Forrester, 2016.

[2] Zero Trust Architecture, NIST SP 800-207, 2020 https://csrc.nist.gov/pubs/sp/800/207/final

[3] Y.J.Choi, Y.J.Jeong, M.H.Lee, “Zero Trust Standard Model Checklist Based on NIST 7 Tenets“, Review of KIISC, Vol.34, Issue.3, pp.5-12

[4] Vasu Jakkal, “Zero Trust Adoption Report,”Microsoft Security, 2021.

[5] Delinea, “What is Zero Trust and Zero TrustExtended (ZTX)https://delinea.com/what-is/zero-trust-and-zero-trust-extended.

[6] https://www.trendmicro.com/ko_kr/what-is/what-is-zero-trust/secure-access-service-edge.html

[7] W.H.Yoon, H.J.Lee, “For the difficult and arduous journey of zero trust, ”2023 Second Cybersecurity Coalition Report“, pp.28-43, 2023.

[8] National Institute of Standards and Technology, “Implementing a Zero Trust Architecture,” NISTSP 1800-35, 2022.

[9] K.H.Lee “IA Study on the Infringement Incident Response Curriculum Model in IoT Environmentt”. Journal of Internet of Things and Convergence, Vol.9, No.3, pp.55-60, 2023.

[10] H.W.Kim. “Intrusion response methods in the Internet of Things (IoT) environment”. Journal of the Korea Institute of Information Security and Cryptology, Vol.28, No.4, 739-749, 2018.

[11] J.H.Lee, “Security threats and response methods in the Internet of Things (IoT) environment”. Journal of the Korea Institute of Information Security and Cryptology, Vol.27, No.4, 697-706. 2017.

[12] Y.M.Park, “Training program model for intrusion response in the Internet of Things (IoT) environment”. Journal of the Korea Institute of Information Security and Cryptology, Vol.29, No.4, 795-804. 2019.

[13] "The Internet of Things (IoT): A Security Perspective", by Andrew S. Tanenbaum and Maarten van Steen, in "The New Internet", edited by Andrew S. Tanenbaum and Maarten van Steen, 2010.

[14] "Security in the Internet of Things", by Richard E. Smith, in "The Internet of Things: A Systems Perspective", edited by Richard E. Smith, 2015.

[15] K.H.Lee, “A Study on a Project-based Blockchain Web Developer Education Model Customized for Companies”, Journal of Internet of Things and Convergence, Vol.8, No.4, pp.77-83, 2022.

[16] M.G.Lee, “A Development of Curriculum for Information Security Professional Manpower Training”, Journal of the Institute of Electronics and Information Engineers, Vol.54, No.1, pp.46-52, 2017.

이 근 호(Keun Ho Lee) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
■ 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
침해사고대응, 융합보안, 개인정보보호, 블록체인