https://doi.org/10.33778/kcsa.2021.21.3.025

Cloud HSM와 edge-DRM Proxy를 활용한 안전한 원격근무 환경 강화 연구

김 현 우*, 이 준 혁*, 박 원 형**

요 약

현재 코로나-19 팬데믹 현상으로 인해 기업이나 기관에서는 원격근무를 제공하는 상황에서 안전한 근무환경을 구축하기 위해 논리적 망 분리 기술 중 하나인 가상화 데스크톱 기술을 도입하고 있다. 가상화 데스크톱 기술을 도입함에 따라 기업이나 기관에서는 망분리 환경을 보다 안전하고 효과적으로 운영할 수 있게 되었으며, 업무망에 신속하고 안전하게 접근해 업무 효율성과 생산성을 높일 수 있게 되었다. 그러나 가상화 데스크톱 기술을 도입함에 있어, 높은 사양의 서버와 스토리지, 라이선스의 비용적인 문제가 있으며, 운용 및 관리적인 측면에서의 보완이 필요한 실정이다. 이에 대응하기 위한 방안으로 기업이나 기관에서는 클라우드 컴퓨팅 기반의 기술인 가상 데스크톱 서비스(DaaS, Desktop as a Service)로 전환하는 추세이다. 하지만 클라우드 컴퓨팅 기반의 기술인 가상 데스크톱 서비스에서 공동책임모델은 사용자 접근 통제와 데이터 보안은 사용자에게 책임이 있다. 이에 본 논문에서는 가상 데스크톱 서비스 환경에서 공동책임 모델을 근거로, 사용자 접근 통제와 데이터 보안에 대한 개선 방안으로 클라우드 기반 하드웨어 보안 모듈(CloudHSM)과 edge-DRM Proxy를 제안한다.

Enhancement of a Secure Remote Working Environment using CloudHSM and edge-DRM Proxy

Hyunwoo Kim*, Junhyeok Lee*, Wonhyung Park**

ABSTRACT

Due to the current COVID-19 pandemic, companies and institutions are introducing virtual desktop technology, one of the logical network separation technologies, to establish a safe working environment in a situation where remote work is provided. With the introduction of virtual desktop technology, companies and institutions can operate the network separation environment more safely and effectively, and can access the business network quickly and safely to increase work efficiency and productivity. However, when introducing virtual desktop technology, there is a cost problem of high-spec server, storage, and license, and it is necessary to supplement in terms of operation and management. As a countermeasure to this, companies and institutions are shifting to cloud computing-based technology, virtual desktop service (DaaS, Desktop as a Service). However, in the virtual desktop service, which is a cloud computing-based technology, the shared responsibility model is responsible for user access control and data security. In this paper, based on the shared responsibility model in the virtual desktop service environment, we propose a cloud-based hardware security module (Cloud HSM) and edge-DRM proxy as an improvement method for user access control and data security.

Keywords : Daas(Desktop as s Service), CloudHSM, edge-DRM proxy, Remote Work

접수일(2021년 08월 27일), 수정일(2021년 09월 13일), 게재확정일(2021년 9월 30일)

* 상명대학교 정보보안공학과 학부생 (주저자)
** 상명대학교 정보보안공학과 부교수 (교신저자)

1. 서 론

최근 코로나-19 팬데믹 현상으로 인해 전세계적으로 원격근무 서비스를 도입한 기업이 약 43% 증가하였다. 원격근무 서비스를 도입한 결과, 업무 생산성 향상과 비용 절감 등 이점을 가지게 되면서 코로나-19 이후에도 기업이나 기관들이 활용할 것으로 전망하고 있다[1][2][3]. 이에 기업이나 기관들에서는 원격근무 서비스를 제공하는 상황에서 안전한 근무환경을 구축하기 위해 논리적 망분리 기술 중 하나인 가상화 데스크톱 기술을 도입하고 있다[4]. 가상화 데스크톱 기술을 도입함에 따라 기업이나 기관에서는 망 분리 환경을 보다 안전하고 효과적으로 운영할 수 있게 되었으며, 업무망에 신속하고 안전하게 접근하게 됨으로써 업무 효율성과 생산성을 높일 수 있게 되었다.

그러나 가상화 데스크톱 기술을 도입함에 있어, 많은 VD들에게 서비스를 제공하는 과정에서, 높은 사양의 서버와 스토리지, 라이선스 등 비용적인 문제가 발생한다. 또한 데이터 중앙화 관리를 하는 가상화 데스크톱 기술 특성상, 기업 자체에서 관리해야 할 보안 요소들이 증가한다는 문제가 발생한다. 이러한 문제점에 대응하기 위한 방안으로, 기업이나 기관에서는 클라우드 컴퓨팅 기반 기술인 가상 데스크톱 서비스(DaaS)를 도입하는 추세이다. 글로벌 리서치 전문기관인 가트너에 의하면 글로벌 가상화 데스크톱 시장 규모가 '20년 110억 달러에서, '25년 255억 달러로 연평균 16.1% 증가할 것으로 전망하고 있다[5]. 그러나 공유책임모델을 지니고 있는 클라우드 서비스에서는 인프라에 대한 보안은 책임지지만, 사용자 접근 통제 및 데이터 보안은 사용자에게 책임이 있다.

따라서 본 논문에서는 사용자 접근 통제와 데이터 보안에 대한 강화 방안으로 클라우드 기반 하드웨어 보안 모듈(CloudHSM)과 edge-DRM Proxy를 제안한다. 논문의 구성은 다음과 같다. 2장은 관련 기술을 소개한다. 3장은 강화 방안을 설명한다. 4장은 결론을 요약하고 향후 강화 방향을 제시한다.

2. 관련 연구

2.1 사이버 보안 위협

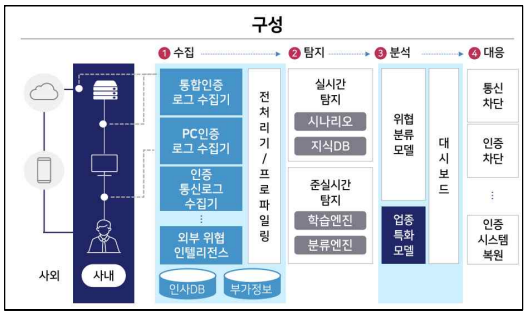
최근 코로나-19로 인해 원격근무로 전환하는 기업이 증가함에 따라 사이버 공격의 볼륨과 심각성 및 범위 또한, 증가하였다. 글로벌 보안 기업 탈레스의 2021 탈레스 글로벌 데이터 위협 보고서에 따르면, 기업의 42%는 지난해 보안 침해를 겪은 것으로 나타났다. 이는 2019년의 21%에서 약 두 배로 증가한 수치로, 위협 환경이 변화함에 따라 사이버 보안 위협이 증가하고 있다. 그러나 코로나-19 팬데믹 기간 동안 원격근무로 인한 보안 위협 증가에도 불구하고, 42%의 기업들은 자사의 보안 인프라가 코로나 19로 야기된 위협에 대응할 준비가 되어있지 않다고 응답했다[6].

이러한 사이버 보안 위협으로부터 기업을 보호하기 위해서 제로 트러스트 네트워크 엑세스, 클라우드 기반의 액세스 관리 등에 대한 투자를 진행하고 있다. 그러나 대부분의 조직들에서 클라우드 인프라의 사용이 증가하고 있음에도 불구하고, 개인정보보호 및 데이터 보호 규정을 관리함에 있어 한계가 발생하고 있다. 이에 따라서, 클라우드 기반 원격근무 환경 구축에 대한 강화 방안 마련이 요구되고 있다.

2.2 원격근무 환경 구성

기업에서 안전한 원격근무 환경을 구축하기 위해 크게 고려해야 할 사항은 2가지이다. (그림 1)은 안전한 원격근무 환경 구성도이다.

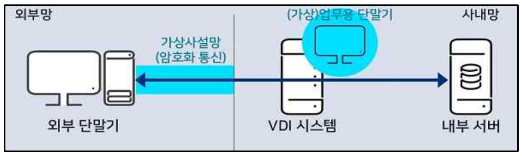
첫 번째로, 사용자 접근 통제를 하기 위해 기업에서는 접근 통제 및 검사/로깅, 업무시스템 접속관리/차단, 원격접속 모니터링, 사용자 계정 및 권한 관리를 활용한다[7]. 두 번째로, 정보 유출에 대한 방어, 즉 데이터 보안이다. 이에 기업에서는 매체제어, DRM, 캡처 방지, 출력 통제 등을 활용한다[8]. 하지만 원격 근무 환경이 가상화 데스크톱 서비스(DaaS) 기반의 형태로 변화함에 따라 사용자 접근 통제와 데이터 보안의 방식 또한, 운용적인 측면에서 변화가 요구된다.



(그림 1) 안전한 원격근무 환경 구성도

2.3 가상화 데스크톱(VDI) 구성도

현재 많은 기업이나 기관에서는 안전한 원격근무 서비스를 제공하기 위해 가상화 데스크톱(VDI) 기술을 도입하고 있다. 가상화 데스크톱(VDI) 구성도는 (그림 2)과 같다.



(그림 2) 데스크톱 가상화(VDI) 구성도

가상화 데스크톱(VDI) 방식은 외부 단말기에서 가상화 데스크톱(VDI)의 가상 업무용 단말기를 경유하여 내부망에 접속하는 것이다. 가상화 데스크톱(VDI)은 사내 공개망 또는 내부 업무망에 위치할 수 있으며, 가상 데스크톱 서비스(DaaS)에서의 활용도 가능하다[9].

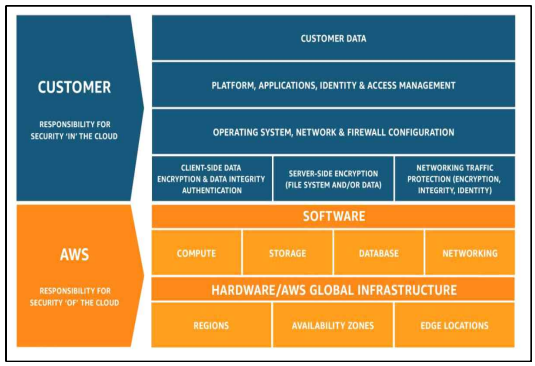
2.4 가상 데스크톱 서비스(DaaS)

가상 데스크톱 서비스(DaaS)란 퍼블릭 또는 프라이빗 클라우드 서비스를 통해 가상 애플리케이션 및 데스크톱 서비스를 제공하는 서비스이다. 이 서비스는 기존의 가상화 데스크톱(VDI) 방식과 다르게 클라우드 컴퓨팅에 기반이 되어 호스팅된 가상화 데스크톱(VDI)의 한 형태이다[10].

가상 데스크톱 서비스(DaaS)를 도입함으로써 기업이나 기관에서는 자본 비용을 절감시키고, 가상화 데스크톱 인프라(VDI) 배치 및 관리 필요성을 최소화 한다는 이점을 갖는다. 또한, 다수의 기업이나 기관들의 상황과 환경에 고려한다는 유연성과 즉각적인 대응이 가능하다는 점과 더불어 데이터가 클라우드 저장소에 저장 및 관리되어 데이터를 안전하게 보안할 수 있다. 이러한 이점을 통해 기존의 가상화 데스크톱(VDI)의 문제점을 보완할 수 있다[11].

2.5 공동 책임 모델

가상 데스크톱 서비스(DaaS)를 이용할 때 공급자와 사용자 사이에서 공동 책임이 있다. (그림 3)는 AWS의 공동책임모델이다.



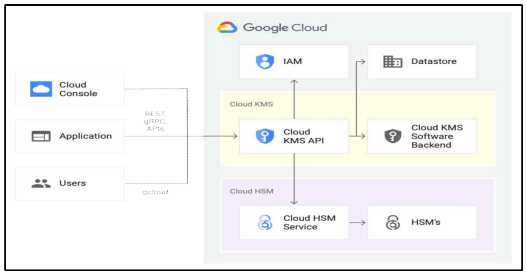
(그림 3) AWS 공동책임모델

AWS 공동책임모델에서 공급자는 제공되는 모든 서비스를 실행하는 인프라를 보호할 책임이 있다. 이 인프라는 가상 데스크톱 서비스(DaaS)에서 실행하는 하드웨어, 소프트웨어, 네트워킹 및 시설로 구성이 된다. 하지만 사용자 접근 통제와 데이터 보안은 사용자에게 책임이 있다[12]. 따라서, 본 논문에서는 사용자 접근 통제와 데이터 보안에 대한 강화 방안으로 클라우드 기반 하드웨어 보안 모듈(CloudHSM)과 edge-DRM Proxy를 제안한다[13][14][15][16][17][18].

3. Cloud HSM 활용한 원격 근무환경 강화 방안

3.1 클라우드 기반 하드웨어 보안 모듈(Cloud HSM)을 활용한 사용자 인증 보안 강화 방안

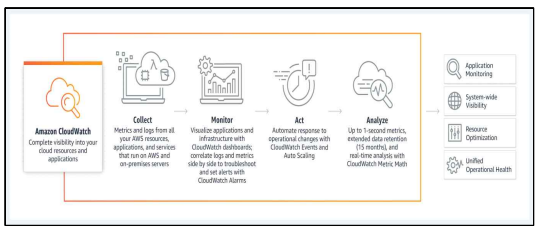
현재 기존의 사용자 인증 보안 시스템은 소프트웨어적 기법에 기반을 두고 있어 공격 방법이 진화함에 따라 끊임없는 보완이 필요하다는 단점이 존재하여 근본적인 해결책이 필요한 실정이다[13]. 이에 하드웨어 인증 방법으로 클라우드 기반 하드웨어 보안 모듈(CloudHSM)을 활용한 사용자 인증 보안 강화 방안을 제시하고자 한다. (그림 4)는 Google의 CloudHSM 구성도이다.



(그림 4) Google의 CloudHSM 구성도

CloudHSM이 원격근무 환경에 도입될 경우 인증 및 권한 부여의 기능을 활용하여 사용자 인증 보안 강화를 할 수 있을 뿐만아니라, 인증기관(CA)를 클라우드 서비스에 둠으로써 조직의 인증서를 발행하는 발생 인증기관(CA)의 역할을 안전하게 수행할 수 있다. 또한 인증 및 권한 부여를 수행하는 IAM(Identity And Access Management)을 사용하면 다른 사용자, 서비스 및 애플리케이션이 리소스를 제한된 방식으로 사용할 수 있다. 이를 통해 보안 자격 증명을 공유하지 않아도 된다는 장점이 있다.

또한, CloudHSM 도입시 대표적인 모니터링 서비스인 AWS의 CloudWatch같은 기능을 활용하면, 기존의 원격근무 환경과 같이, 원격접속 모니터링 및 검사/로깅이 가능하다. CloudWatch 작동 방식은 (그림 5)와 같다.



(그림 5) AWS의 CloudWatch 작동 방식

CloudWatch 서비스를 사용하면, CloudHSM에서 발생하는 모든 로그들을 일관된 사용자 지정 계산을 통하여 이벤트 흐름으로 정렬하고 그룹화하여 시각화할 수 있다. 이러한 기능을 통해 이상 행위 검사/로깅과 더불어, 원격접속 모니터링을 수행할 수 있다.

3.2 클라우드 기반 하드웨어 보안 모듈(Cloud HSM)을 활용한 사용자 인증 보안 검증

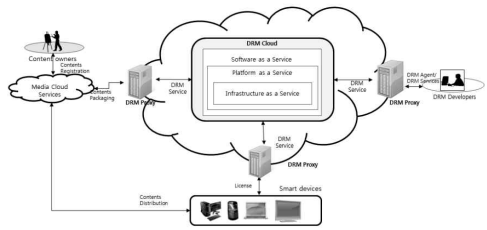
현재 사용자 인증 보안을 강화하기 위해 Cloud HSM을 제공하는 Microsoft, Amazon, Google 등 대부분의 기업들은 암호화 모듈의 유효성을 검사하는데 사용되는 미국 정보 컴퓨터 보안 표준인 FIPS 140-2 level3를 인증받았다. FIPS 140-2 level3란 침입 방지, 신원 기반 인증, 물리적 또는 논리적 분리, 운영체제 요구 사항을 충족하는 수준이며, 대부분의 조직에서 강력한 데이터 보호를 보장하기 위해 요구되는 수준이다. 또한, CloudHSM을 도입 시, 다른 보안 시스템의 연동도 유연하기 때문에 높은 보안성을 준수할 수 있다.

4. edge-DRM Proxy 활용한 원격 근무환경 강화 방안

4.1 edge-DRM Proxy를 활용한 데이터 보안 강화

현재 클라우드 서비스에서는 암호화 및 로깅 기능 등 기본적인 데이터 보안은 제공하고 있지만, 데이터 유출에 대한 책임은 사용자에게 있다. 사이버 보안 위협의 이를 해결하기 위해 기존 가상화 데스크톱(VDI) 환경에서의 사용자는 데이터 접근 제어를 하기 위해 디지털 저작권 관리(DRM, Digital Rights Management)을 도입하였다. 하지만 가상 데스크톱 서비스(DaaS) 도입 시, 서로 다른 서비스 간의 상호운용성에 문제가 있다. 따라서 본 본문에서는 edge-DRM Proxy를 도입함으로써 상호운용성의 문제를 해결하고 더 나아가 edge-DRM Proxy의 확장성을 활용하여

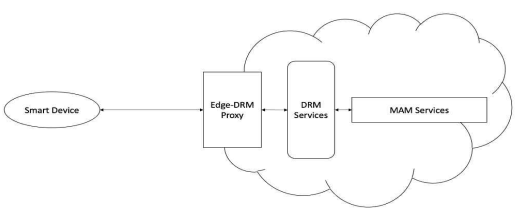
클라우드 환경에서 모바일 앱 관리 기술인 MAM 기술과 융합한 edge-DRM Proxy 모델을 제안한다. edge-DRM Proxy란 DRM 서비스를 클라우드 환경에서 사용하기 위해 사용자 측면인 엔드포인트 단에서 중간자 역할을 수행하는 proxy를 도입하여 DRM 서비스의 상호운용성을 해결하고자 제안된 모델이다. (그림 6)는 edge-DRM Proxy의 구성도이다.



(그림 6) edge-DRM Proxy 구성도

edge-DRM Proxy는 클라우드 엔드포인트 단에 구현되어 클라우드 서버에 있는 서비스를 호출하여 사용하는 방식이다. 이러한 구성은 네트워크를 통해 서비스를 호스팅하는 클라우드 특성상 다른 서비스를 사용하기에 확장이 유연하고 용이하다. 따라서 본 본문에서는 이러한 edge-DRM Proxy의 확장성을 활용하여 가상 데스크톱 서비스(DaaS) 환경에서 MAM 기술을 융합하고자 한다.

MAM이란 모바일 앱 관리 기술로, 원격근무 환경에서 단말기 내의 사용되는 앱에 대한 접근 및 사용을 프로비저닝하고 제어하는 클라우드 소프트웨어 서비스이다. MAM 기술 도입 시, 가상 데스크톱 서비스(DaaS) 환경에서는 회사와 개인 앱을 분리하고, 원격으로 관리 및 업데이트함에 따라 데이터 보안을 강화할 수 있다. (그림 7)은 edge-DRM Proxy와 MAM 기술을 융합한 모델이다.



(그림 7) edge-DRM Proxy와 MAM 기술을 융합한 모델

edge-DRM Proxy와 MAM 기술을 융합한 모델을 가상 데스크톱 서비스(DaaS) 환경에 도입 시, 기업의 내부 데이터를 DRM 서비스로 보호 및 추적한다. 또한, 기존의 DRM 서비스의 단점인 관리 용이성과 주기적인 업데이트를 MAM 기술을 통해 보완할 수 있다. 더 나아가 일차적으로 DRM 서비스를 통해 데이터 자체 보안을 강화할 수 있고, 이차적으로 MAM 기술을 통해 사용자 디바이스 관리 및 접근 제어를 할 수 있어 데이터 보안을 더욱 강화할 수 있다.

5. 결 론

최근 가상 데스크톱 서비스(DaaS)로 전환하는 기업이 증가함에 따라 기존의 안전한 원격근무 환경 구성도와 공동책임모델을 활용하여 사용자 접근 통제와 데이터 보안에 대한 효과적인 강화 방안을 제안하였다. 본 논문을 통해 두가지 강화 방안을 다음과 제안 한다.

첫 번째, 사용자 인증 보안 강화 방안으로 클라우드 기반 하드웨어 보안 모듈(CloudHSM)을 제안하였다. 이를 활용하면 사용자 인증에 대한 접근 통제, 업무시스템 접속 관리/차단, 사용자 계정 및 권한 관리 기능을 강화할 수 있다. 또한, AWS의 CloudWatch와 같은 기능을 활용하면 이상행위 검사/로깅, 원격접속 모니터링을 수행함으로써 현재 기업이나 기관의 사용자 접근 통제의 이점을 가져올 수 있을 것으로 기대한다. 두 번째, 데이터 보안 강화 방안으로 edge-DRM Proxy의 활용을 제안하였다. 이를 사용하면 상호운용성의 문제를 해결하고 더 나아가 edge-DRM Proxy의 확장성을 활용하여 클라우드 환경에서 모바일 앱 관리 기술인 MAM 기술과 융합한 edge-DRM Proxy 모델을 사용함으로써 기존의 DRM 서비스에서 제공하는 데이터 보호 및 추적과 더불어, 기존의 DRM 서비스 단점인 관리 용이성과 주기적인 업데이트를 MAM 기술을 통해 보완할 수 있다. 이를 통해 기업이나 기관에서는 내부정보유출 사고를 방지할 수 있고 DRM 클라우드를 통해 내부정보에 대한 역추적성을 확보할 수 있을 것으로 판단

된다. 향후 추가 연구로는 현재 기업이나 기관에서의 보안사고는 대다수 내부정보유출이기 때문에 이를 보완하기 위해 제로 트러스트 기반의 연구가 필요하다. 또한, 사용자 인증과 데이터에 한정하여 강화 방안을 제안하였으나, 이를 확장하여 서버, 네트워크, 응용프로그램 등에 대한 확대 적용 검토가 필요하다.

참고문헌

[1] Cisco. "Future fo Secure Remote work Report". 2020. pp. 5.

[2] 정종길, 업무 환경 디지털 전환, 안정성·보안 갖춘 VDI가 적격, https://www.comworld.co.kr/news/articleView.html?idxno=49903, 컴퓨터월드, 2020.7.

[3] 한컴-아마존 '클라우드PC' 연합군 뜬다[한국경제] 기사, https://www.hankyung.com/it/article/2021033096581, 2021.3.

[4] THALES. "2021 data threat report apac edition a4 ko." 2021. pp.5-8.

[5] 한현희, "원격 근무 환경에서의 계정 보안 강화", Cyber security Conference 2021 pp.7-18.

[6] 조원용, "차세대 방화벽을 이용한 안전한 원격근무 환경 구성", Cyber security Conference 2021 pp.6.

[7] 재택 근무 보안 방안, 안랩의 해답은?, https://blog.naver.com/softinfoblog/222262011172, 안랩, 2021.3.

[8] 서비스형 데스크탑(DaaS)이란?, https://www.critix.com/ko-kr/glossary/what-is-desktop-as-a-service-dass.html, 시트릭스, 2020.

[9] K-ICT 클라우드혁신센터, 2020년 5월 7일 수정, 2021년 8월 24일 접속, https://www.cloud.or.kr/software/market-case/?pageid=8&mod=document&uid=550.

[10] 공동 책임 모델, https://aws.amazon.com/ko/compliance/shared-responsibility-model/, AWS, 2021.

[11] 이상현. "클라우드 환경에서의 사용자 인증 방안에 관한 연구" 국내석사학위논문 숭실대학교 정보과학대학원. 2016. pp.1-37.

[12] Cloud HSM 아키텍처, https://cloud.google.com/security/cloud-hsm-architecture, AWS, 2021.6.

[13] AWS 클라우드상의 관리형 하드웨어 보안 모듈(HSM), https://aws.amazon.com/ko/cloudhsm/, AWS, 2021.

[14] AWS 및 온프레미스에서 AWS 리소스 및 애플리케이션의 관찰 기능, https://aws.amazon.com/ko/cloudwatch/, AWS, 2021.

[17] 이혜주, 허창수, 서창호, 신상욱. "DRM 클라우드 서비스를 위한 DRM Proxy 설계 및 구현 ". 정보처리학회논문지. v.2 no.12. 2013. pp. 553 - 560.

[18] 박장수. "내부정보유출 방지를 위한 통합 모니터링에 관한 연구." 국내박사학위논문 순천향대학교, 2017. pp.1-49.

[저자소개]

김 현 우 (Hyunwoo Kim)

현재 상명대학교 정보보안공학과 학부생

email : rmrehd604@gmail.com

이 준 혁 (Junhyeok Lee)

현재 상명대학교 정보보안공학과 학부생

email : alexlee5151@gmail.com

박 원 형 (Wonhyung Park)

2002년 서울과학기술대 산업정보시스템 학사

2005년 서울과학기술대 정보산업공학과 석사

2009년 경기대학교 정보보호학 박사

2015년 성균관대학교 컴퓨터교육학 박사수료

2012년~2020년 극동대학교 사이버보안학과 교수/학과장

현재 상명대학교 정보보안공학과 부교수

email : whpark@smu.ac.kr