Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.1, Feb. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.1.83

제로트러스트 기반의 원격 근무 환경을 구축하기 위한 보안요구사항 분석 연구*

김 해 나,[1†] 김 예 준,[1] 김 승 주[2‡]
[1,2]고려대학교 (대학원생, 교수)

A Study on the Security Requirements Analysis to Build a Zero Trust-Based Remote Work Environment*

Hae-na Kim,[1†] Ye-jun Kim,[1] Seung-joo Kim[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

최근 클라우드의 사용량이 해마다 증가하고 기업 내 원격 근무가 새로운 근무 형태 중 하나로 자리 잡으면서 클라우드 기반 원격 근무 환경의 보안이 중요해졌다. 내부 네트워크 안에 있는 모든 것은 안전하다고 가정하는 기존의 경계 기반 모델의 한계로 인해 제로트러스트 도입이 요구되고 있다. 이에 따라 NIST 및 DoD는 제로트러스트 아키텍처 관련 표준을 발간하였지만, 해당 표준의 보안요구사항은 추상적인 수준에서 논리적 아키텍처만을 기술하고 있다. 따라서 본 논문에서는 OpenStack 클라우드에 대한 위협모델링을 수행하여 NIST 및 DoD 표준에 비해 보다 상세한 보안요구사항을 제시하고자 한다. 이후 본 연구팀은 해당 요구사항에 대한 검증을 위해 상용 클라우드 서비스들에 대한 보안성 분석을 수행하였다. 보안성 분석 수행 결과 본 연구팀에서는 각 클라우드 서비스가 만족하지 못하는 보안요구사항을 식별하였다. 본 연구팀은 제로트러스트가 적용된 클라우드 서비스에 대한 잠재적 위협과 대응 방안을 제안하였으며, 이를 통해 안전한 제로트러스트 기반 원격 근무 환경을 구축하는데 도움이 되고자 한다.

ABSTRACT

Recently, as the use of the cloud increases year by year and remote work within the enterprise has become one of the new types of work, the security of the cloud-based remote work environment has become important. The introduction of zero trust is required due to the limitations of the existing perimeter security model that assumes that everything in the internal network is safe. Accordingly, NIST and DoD published standards related to zero trust architecture, but the security requirements of that standard describe only logical architecture at the abstract level. Therefore, this paper intends to present more detailed security requirements compared to NIST and DoD standards by performing threat modeling for OpenStack clouds. After that, this research team performed a security analysis of commercial cloud services to verify the requirements. As a result of the security analysis, we identified security requirements that each cloud service was not satisfied with. We proposed potential threats and countermeasures for cloud services with zero trust, which aims to help build a secure zero trust-based remote working environment.

Keywords: Zero Trust, Cloud System, Remote Work System, OpenStack, Threat Modeling

Received(11. 22. 2023), Modified(01. 18. 2024), Accepted(01. 18. 2024)

* This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2021-0-00613, Zero Trust technology based access control and abnormal event analysis technology development for enterprise network protection in the untact era)

† 주저자, haena0114@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

지난 코로나 19 대유행(pandemic)에 따라 전 세계적으로 재택근무가 급속히 확산되었고 원격 근무가 일하는 방식의 새로운 기준으로 자리 잡았다. 현재는 코로나 19 앤데믹 시대로 접어들었지만 조직원의 만족도 향상, 조직의 생산성 제고 등을 위해 원격 근무는 하나의 근무 형태로 자리 잡았다. 이와 같이 원격 근무 형태의 확장과 관련하여 마이크로소프트 최고경영자 사티아 나델라는 연례 개발자 컨퍼런스에서 "2년이 걸릴 디지털 트랜스포메이션이 2개월 만에 이뤄졌다"고 언급하였다[1]. 또한 미국의 정보 기술 연구 및 자문 회사인 가트너에서는 2023년 전 세계 퍼블릭 클라우드 서비스에 대한 최종 사용자 지출액이 2022년 대비 21.7% 증가한 5,974억 달러(약 791조)에 이를 것으로 전망했다[2].

기존의 클라우드 시스템은 대부분 경계 기반 보안 모델(perimeter security model)을 기반으로 보호받기 때문에, 최근 보고되는 정교화된 사이버 공격에 취약하다는 발표가 이어지고 있다. 대표적인 사례가 랩서스 해킹 그룹의 사이버공격이다. 마이크로소프트, 엔비디아, 삼성 등을 포함한 여러 IT 대기업의 기밀정보를 탈취했다고 알려진 랩서스(lapsus$) 해킹 그룹은 다양한 종류의 사이버공격을 활용하였다. 먼저 해당 그룹은 피싱, 스미싱 등의 사회 공학적 기법을 통해 공격하고자 하는 기업 내 임직원의 계정정보를 수집하였다. 이후, 해당 해킹 그룹은 수집된 정보를 바탕으로 정상적인 사용자인 척 위장하여 기업 망에 접속하였다. 그 후, 해당 해킹 그룹은 기업 내 임직원들이 업무상 사용하는 클라우드 기반의 플랫폼인 컨플루언스, 지라, 깃랩 등의 취약점을 악용하여 자신이 접속했을 당시 권한보다 과도한 권한을 획득하여 사내 기밀 정보에 접근하였다[4]. 이런 것이 가능했던 이유는 경계 기반 보안 모델은 과거에 인증된 사용자에게는 추가적인 인증이 별도로 요구되지 않기 때문이다. 일반적으로 경계 기반 보안 모델은 보호하고자 하는 시스템에 접근하는 개체를 내부자와 외부자로 구분한다. 이때 외부자가 시스템 내부로 접속을 시도하는 경우, 경계 기반 보안 모델에서는 외부자의 신원에 대해 인증이 수행된다. 만약 신원 인증이 정상적으로 완료되는 경우, 경계 기반 모델은 해당 사용자를 항상 신뢰하게 된다. 따라서 랩서스 그룹의 해킹 사례에서 알 수 있듯이 경계 기반 보안 모델은 공격자가 시스템에 접속하는 경우, 이후 수행하는 이상 행위들을 탐지하는 것이 매우 제한된다. 이에 따라 기존 경계 기반 모델의 한계를 보완하기 위해 제로트러스트 기반의 보안 모델이 적용된 시스템의 필요성이 대두되었다. 제로트러스트는 2010년 보안 관련 리서치 기관인 Forrester Research의 제로트러스트 관련 보고서에서 처음으로 정의되었다[5]. 제로트러스트는 문구에서 알 수 있듯이 "아무도 신뢰하지 않는다"라는 개념을 가지고 있으며, 외부자뿐만 아니라 시스템 내부에 접속한 사용자에 대해서도 무조건적으로 신뢰하지 않고 지속적인 모니터링을 통해 신원을 검증한다는 개념이다. 제로트러스트는 이후에도 꾸준히 연구되고 발전되고 있으며, NIST(National Institute of Standards and Technology), DoD (Department Of Defense), NSA(National Security Agency), CISA(Cybersecurity and Infrastructure Security Agency)와 같은 기관들을 통해 표준화되고 있다. 대표적인 가이드라인은 2020년에 발표된 "NIST Special Publication 800-207: Zero Trust Architecture"로, 기업 및 연방 기관을 위한 '제로트러스트 아키텍처'와 제로트러스트 모델의 구현에 있어 가이드라인이 되는 '7가지 원칙'을 제시하고 있다[6]. 그러나 해당 문서에서는 추상적인 수준에서의 논리적 아키텍처만이 기술되어 있다. 보안요구사항이 구체적이지 않을 경우에는 제품 개발의 자유도는 높아질 수 있지만, 개발자나 조직의 보안 전문가가 보안요구사항을 서로 다르게 해석할 여지가 존재한다. 이로 인해 각자의 이해에 따라 구현된 시스템에 일관성이 없는 보안 정책이 적용될 수 있다. 또한, 원격 근무 환경에서 보안 사고가 발생할 경우, 불충분한 보안요구사항으로 인해 사고 대응이 늦어지고 비효율적으로 이루어질 수 있다.

이에 따라 본 연구팀은 클라우드 기반의 원격 근무 환경에 제로트러스트 기반의 보안 모델을 적용하는 데 필요한 상세화된 보안요구사항을 제안한다. 클라우드 기반 원격 근무 환경 구축 시 보안요구사항을 고려하는 것은 중요하다. 클라우드 환경은 다수의 사용자가 동시에 서비스를 이용하는 환경이기 때문에 기업의 내부 자원이 외부로부터 안전하게 보호되어야 한다. 이를 위해 본 연구팀은 오픈소스 클라우드 서비스 중 Fortune 100대 기업 내에서 시장 점유율이 가장 높은[8] OpenStack을 선정하여 위협모델링을 수행하였다. 이후 위협모델링 수행 결과를 바탕으로 본 연구팀은 클라우드 기반의 원격 근무 환경에 제로트러스트 기반의 보안 모델을 적용하는데 필요한 상

세 보안요구사항을 도출하였다. 또한, 도출한 보안요구사항을 바탕으로 제로트러스트 원칙이 적용된 클라우드 서비스로 알려진 Microsoft Azure, Amazon Web Service, Google Cloud에 대한 보안성 분석을 수행하였다. 본 논문에서의 보안성 분석은 각 클라우드 서비스 분석 결과와 도출된 보안요구사항을 비교하는 방식으로 수행되었다. 본 연구팀은 보안성 분석 결과 각 서비스에서 일부 보안요구사항이 만족하지 못함을 확인했으며, 이는 잠재적인 보안문제가 발생될 수 있다는 것을 의미한다. 따라서 본 논문에서는 분석 대상 서비스에서 발생될 수 있는 보안 문제점 및 이를 완화하기 위한 방안을 제안하였다. 도출된 보안요구사항과 실제 서비스의 잠재적 위협 및 완화방안은 제로트러스트가 적용된 클라우드 서비스를 개발하는 개발자가 보안성이 높은 클라우드 서비스를 구현할 수 있도록 한다. 이를 통해 클라우드 서비스 제공자는 사용자에게 보다 안전하고 신뢰성 있는 환경을 제공할 수 있다. 본 논문은 다음과 같이 구성되어 있다. 먼저 본 논문의 1장에서는 연구의 배경과 필요성, 이후 2장에서는 제로트러스트 관련 학술 동향, 표준화 동향, 상용클라우드 서비스 동향에 대해 설명하고, 3장에서는 OpenStack 클라우드 대상의 위협모델링을 수행하여 제로트러스트 원칙이 적용된 상세한 보안요구사항을 제시한다. 4장에서는 NIST 및 DoD 보안요구사항과 본 연구팀이 도출한 상세한 보안요구사항을 기반으로 기존 상용 클라우드 서비스에 대한 보안성 분석 결과를 제시한다. 마지막으로 5장에서는 본 연구의 결론을 짓고 마무리한다.

II. 제로트러스트 연구 동향

2.1 관련 학술 연구 동향

2010년, Forrester Research의 John Kindervag는 “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security”에서 제로트러스트란 개념을 처음으로 정의하였다[5]. 해당 문서에 따르면 제로트러스트 모델이란 네트워크상 존재하는 모든 주체를 신뢰하지 않고 끊임없이 신원을 검증하는 보안 모델을 의미한다. 2014년, Rory Ward와 Betsy Beyer는 USENIX(advanced computing systems association)에서 BeyondCorp: A new approach to enterprise security를 발표하였다[9]. 이는 마이크로소프트에서 제안한 네트워크 시스템으로 제로트러스트 기반의 보안 모델이 적용된 최초의 사례이다. 해당 연구에서 제시된 보안 모델은 신뢰할 수 없는 네트워크에서 VPN(Virtual Private Network)을 사용하지 않아도 직원들이 업무를 안전하게 수행할 수 있도록 한다. 2018년, Bryan Zimmer는 USENIX에서 LISA: A practical zero trust architecture를 발표하였다[11]. 이는 넷플릭스(netflix)에 도입된 제로트러스트 기반의 보안 모델로 기존에 비해 간단한 원칙을 기반으로 안전한 원격 근무 환경을 제공할 수 있다는 장점을 가진다. 2020년, T. Dimitrakos 등은 제로트러스트 모델을 IoT 환경에 적용하고, 연속적 권한 부여를 통해 신뢰를 구축하고 유지하는 연구를 수행하였다. 홈 네트워크 내 IoT 디바이스에 대한 인증 및 접근 정책 모델인 제로트러스트 기반의 ABAC(Attribute-Based Access Control) 및 UCON+(Usage Control+)를 제안하며 Trust Level Evaluation Engine(TLEE) 기반의 접근제어 모델을 통해 제로트러스트 아키텍처를 제시하였다[12]. 2021년, S. Mandal 등은 클라우드를 기반으로 하는 제로트러스트기반 접근 제어 정책을 제안하였다. 해당 연구에서는 MAC 스푸핑 공격으로부터 안전한 네트워크를 구축하기 위한 제로트러스트 기반의 새로운 접근제어 정책을 제시하였다[13]. 2022년, P. García Teodoro 등은 사용자와 디바이스의 보안 프로필을 기반으로 한 새로운 제로트러스트 네트워크 접근 제어 방식에 관한 연구를 수행하였다. 해당 연구에서는 기업 네트워크 및 서비스 제공업체의 보안을 강화하기 위해 제로트러스트 기반의 새로운 접근제어 정책으로 SADAC(Security Attribute-based Dynamic Access Control)를 제안하며 네트워크 및 통신 환경의 위험을 최소화하여 보안성을 향상시킬 수 있다고 제시하였다[14]. 2023년, Nisha T. N. 등은 5가지 보안속성을 고려하여 접근제어 및 인증과 관련된 3가지 보안계층을 기반으로 하는 제로트러스트 아키텍처를 제안하고 이를 구현하기 위한 6단계 프레임워크를 제시하였다[15].

이처럼 제로트러스트에 대한 많은 학술 연구가 이루어지고 있지만, 각 연구들은 네트워크, 시스템 내 접근제어 모듈 등에 한정하여 제로트러스트 원칙을 적용하였다. 그러나 제로트러스트 아키텍처는 단일 솔루션으로 구축할 수 있는 것이 아니기 때문에 일부 모듈에만 제로트러스트를 적용하는 것은 적절치 않다. 따라서 본 연구팀은 전반적인 클라우드 환경을

고려하여 기존 상용 클라우드 서비스에 대한 보안성 분석을 수행하여 보다 상세한 제로트러스트 기반의 보안요구사항을 제시하고자 한다.

2.2 표준화 동향

2018년 미국은 연방 정부 차원에서 제로트러스트의 원칙을 도입하기 위한 목적으로 Zero Trust/SDN Steering Group을 설립하였으며, 미국 기술산업자문위원회를 통하여 제로트러스트 기술 동향을 연구하기 시작했다[16]. 그 결과 2019년 NIST는 제로트러스트의 중요성을 인식하고 산하 연구 기관을 통해 제로트러스트 기반의 보안 모델을 개발하기 위한 연구를 수행하였다[17]. 이후, NIST는 2020년 8월에 제로트러스트에 대한 정의와 이를 개발하는 데 필요한 원칙 등의 다양한 정보가 포함된 '제로트러스트 아키텍처(Zero Trust Architecture, SP 800-207)' 가이드라인을 발표하였다[6]. 2021년 2월, DISA(Defense Information Systems Agency) 및 NSA는 제로트러스트와 관련된 지침 및 가이드 문서를 발표하였다. DISA와 NSA는 미 국방부의 정보보안 전략과 제로트러스트 기반의 네트워크 보안 모델을 개발하고 이를 운영하기 위한 지침이 포함된 DoD Zero Trust Reference Architecture ver 1.0 지침을 발간하였다[18]. 또한 NSA의 경우, 사이버 공격으로부터 자산을 보호하기 위해 어떻게 기존 보안 모델과 제로트러스트 원칙을 융합할 것인가에 대한 방법이 포함된 Embracing a Zero Trust Security Model 문서를 제안하였다[19]. 그 외에도 2023년 4월, CISA는 Zero Trust Maturity Model을 통해 제로트러스트에 대한 성숙도 모델 2.0을 제안하였다[20]. 이와 같이 제로트러스트에 대한 표준화 연구가 활발하게 수행되고 있다. 제로트러스트를 도입하고자 하는 기업 및 정부, 공공기관에 따라 네트워크 구조, 조직 내 정책, 규정이 모두 다르기 때문에 현존하는 제로트러스트 표준들은 민간 기관에 자율성을 주기위해 추상적으로 기술되어 있다. 그러나 명확하고 구체적인 보안요구사항의 부재로 인해 원격 근무 환경이 안전하게 설계되고 운영되기 어려울 수 있으며 이는 결국 보안 취약점으로 이어질 가능성이 있다. 그러므로 안전한 시스템을 구축하기 위해 보안요구사항은 명확히 하고 구체적으로 기술되어야 할 필요가 있다[21].

2.3 상용 클라우드 서비스 동향

2.3.1 Microsoft Azure

Microsoft는 2010년도부터 클라우드 서비스인 Microsoft Azure를 제공하고 있다. Microsoft Azure에는 '명확한 검증(verify explicitly)', '최소한의 권한 부여(use least privilege access)', '위반 가정(assume breach)'의 제로트러스트 원칙이 적용되어 있다[22]. 명확한 검증은 모든 리소스와 데이터에 항상 권한을 부여하고 사용자 인증을 수행해야 한다는 원칙을 의미한다. 최소권한의 접근은 모든 사용자 및 리소스에게 최소한의 권한만을 부여한다는 원칙을 의미한다. 위반 가정은 사용자가 시스템에 접근하는 위치와 요청하는 자원과 관계없이 "전혀 신뢰하지 않고 항상 확인"하는 원칙이다. Microsoft Azure는 사용자가 시스템에 접근할 때, 발생 가능한 위협 관련 데이터를 분석 및 수집하여 이후 발생할 수 있는 이상 행위를 식별한다. Microsoft는 이러한 원칙들을 기반으로 ID 인증, 엔드포인트 보호, 애플리케이션 보호, 데이터 보호, 인프라 보호, 네트워크 보호, 자동화 및 오케스트레이션 등의 기술을 Microsoft Azure에 적용하고 있다[23].

2.3.2 Amazon Web Service

미국의 Amazon은 데이터 센터를 통해 자사의 클라우드 서비스인 Amazon Web Service를 제공하고 있다. AWS는 IAM(Identity and Access Management) 기능을 통해 고객들의 시스템에 대한 접근을 엄격히 통제하고 있으며, 암호화 및 키 관리 기능도 포함하고 있다. AWS는 물리적 위치에 관계없이 클라우드 서비스 사용자가 AWS에 저장된 자원을 안전하고 사용할 수 있도록 소프트웨어 정의 경계(software defined perimeter)와 가상 사설망(vpn) 관련 기능을 통해 안전한 네트워크 통신 환경을 클라우드 서비스 사용자에게 제공한다. 그 외에도 Amazon Web Service는 클라우드 서비스 사용자들이 안정적이고 효율적인 서비스를 제공받을 수 있도록 사용자 인증, 최소 권한 부여, 마이크로 세그멘테이션, 지속적인 모니터링, 클라우드 서비스 자동화 및 오케스트레이션과 같은 5가지 주요 요소가 포함된 제로트러스트 기반의 클라우드 서비스를 제공한다[24].

2.3.3 Google Cloud

Google은 2011년도부터 클라우드 서비스인 Google Cloud Platform을 제공하고 있다[25]. Google은 앞서 언급한 대로 제로트러스트 기반의 보안 모델인 BeyondCorp를 자사의 서비스에 적용하였다. Google Cloud Platform은 접근 제어 기능을 통해 VPN을 사용하지 않아도 디바이스와 사용자의 자격 증명에 의존하여 기업 리소스에 접근할 수 있도록 한다[26]. Google은 제로트러스트 관점에서 사용자와 디바이스에 대한 인증·접근제어·모니터링 기능을 제공한다. 관련 기능으로는 IAM(Identity and Access Management), IAP(Identity Aware Proxy), Cloud IDS(Intrusion Detection System) 등이 존재한다.

III. 제로트러스트 기반 클라우드 서비스의 보안 요구사항 제안

위협모델링은 여러 기관 및 조직에서 사용하는 방법론으로 여러 소프트웨어 및 시스템을 개발할 때 보안을 초기부터 고려하여 소프트웨어 시스템의 취약점을 식별하고 관리하기 위해 사용된다. 위협모델링을 통해 시스템 내에서 발생가능한 모든 위협을 식별하고 위협을 완화하기 위한 보안요구사항을 도출할 수 있어 여러 연구에서 이를 활용하고 있다[27-29]. 본 장에서는 위협모델링을 수행하여 식별된 클라우드 기반 원격 근무 환경의 보안 위협을 제시한다. 이후, 식별한 보안 위협을 완화하기 위해 제로트러스트 원칙에 입각한 보안요구사항을 제시하고자 한다. 본 연구팀은 앞서 언급한대로 OpenStack을 위협모델링 대상으로 선정하였으며, 위협모델링을 수행하기 위해 OpenStack 기반의 원격 근무 환경을 구축하였다. 본 연구팀은 소프트웨어에 대한 보안성을 분석할 때, 가장 많이 활용되는 위협모델링 방법론인 Microsoft의 STRIDE를 활용하였다. 해당 위협모델링은 총 5개의 세부 단계로 이루어진다[30]. 각 세부 단계에 대한 간략한 수행 활동은 다음과 같다.

1) 데이터 흐름도 작성: 도출된 분석 대상 아키텍처를 분석하여 구성요소 간 데이터 흐름을 중점적으로 시스템 모델 작성
2) 공격라이브러리 수집: 데이터 흐름도 내 구성요소에 대해 현재까지 알려진 위협들을 모두 수집(CVE/CWE/논문/기술문서 등)
3) 위협 분석: STRIDE-per-Element 규칙에 따라 데이터 흐름도 내 각 구성요소에서 발생할 수 있는 잠재적 위협을 모두 도출
4) 공격 트리 도출: 식별된 위협을 바탕으로 분석 대상에서 발생될 수 있는 공격 시나리오들을 트리의 형태로 도출
5) 보안요구사항 도출: 공격 트리 하위 노드에 대응하기 위한 보안요구사항 도출

위협모델링 결과는 아래 절에 순서대로 제시할 예정이다.

3.1 데이터 흐름도 작성

데이터 흐름도는 시스템 구성요소인 프로세스와 프로세스 간 데이터 흐름을 나타낸다. 데이터 흐름도를 통해 분석 대상 시스템 구성을 데이터 흐름의 관점에서 추상화하여 분석 대상 시스템의 구조와 공격 지점을 식별할 수 있다. 분석 대상 시스템을 추상화하여 데이터 흐름도를 작성하는 경우, 분석 결과가 실제 시스템에 동일하게 적용되어야 하는 성질인 건전성(soundness)이 중요하다. 즉, 데이터 흐름도는 분석 대상과 비교했을 때 누락된 부분이 없도록 작성되어야 한다. 이를 위해 데이터 흐름도는 분석 대상과 추상화한 모델 사이에 차이가 발생하지 않도록 모듈의 내부 기능까지 표현되어야 하며, 이를 위해서는 Context Level, Level 0, Level 1의 순서대로 작성되어야 한다. 본 논문에서는 분석 대상 시스템의 구조 및 공격 지점을 파악하기 위해 OpenStack의 아키텍처를 식별하였다[31]. 이후, Context Level, Level 0, Level 1 수준까지의 데이터 흐름도를 작성하였다. 데이터 흐름도는 ▲Entity, ▲Process, ▲Data Store, ▲Data Flow, ▲Trust Boundary의 5가지 구성요소로 구성된다.

Context Level은 분석 대상을 하나의 프로세스로 표현하는 단계에 해당한다. Context level은 개체(사용자, OpenStack 클라우드 서비스)간의 관계

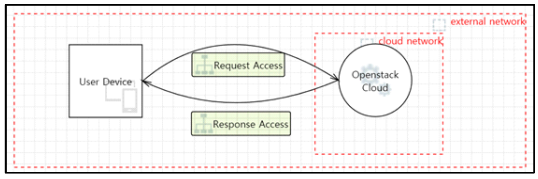

Fig. 1. Context Level DFD

를 간단히 보여준다. Fig 1.은 Context Level의 데이터 흐름도를 나타낸다.

Level 0 데이터 흐름도는 분석 대상의 전반적인 시스템과 주요 구성요소 간의 프로세스를 나타낸다. Level 0 데이터 흐름도는 OpenStack 클라우드의 "OpenStack Logical Architecture"를 기반으로 OpenStack 클라우드의 주요 구성요소를 도출하였다. 그리고 구성요소들 간 오고가는 데이터 흐름을 나타내었다. 각각의 구성요소들은 Level 1 데이터 흐름도에서 OpenStack Github를 기반으로 더욱 상세화된다. Context Level의 데이터 흐름도를 상세화하여 작성한 Level 0 데이터 흐름도는 ▲User Device, ▲Horizon, ▲Keystone, ▲Keystone Backend, ▲Nova, ▲Nova Data Store, ▲VM, ▲Neutron, ▲Neutron Data Store, ▲Glance, ▲Glance DataStore ▲Swift, ▲Swift Data Store, ▲Ring, ▲Cinder, ▲Cinder Data Store 등 총 16가지의 구성요소를 포함한다. Fig 2.는 OpenStack 클라우드의 Level 0 데이터 흐름도를 나타낸다.

Level 1 데이터 흐름도는 각 OpenStack 서비스 구성요소들이 어떻게 동작하는지에 대해 기존 Level 0 데이터 흐름도보다 상세화된다. Level 1 데이터 흐름도는 Level 0의 데이터 흐름도 구성요소에 해당하는 ▲Horizon, ▲Keystone, ▲Nova, ▲VM, ▲Neutron, ▲Glance, ▲Swift, ▲Cinder 등의 구성요소를 상세화하여 총 51개의 구성요소로 이루어져 있다. 대표적인 예로 OpenStack에서 인증 및 인가 서비스를 제공하는 역할을 담당하는 ▲Keystone은 해당 서비스의 다양한 기능들을 지원하는 ▲Keystone Backend, 사용자 및 그룹에 대한 인증을 관리하는 ▲Identity Backend, 사용자의 권한 및 역할을 관리하는 ▲Policy Backend, 모든 OpenStack 서비스에 대한 엔드포인트 URL을 관

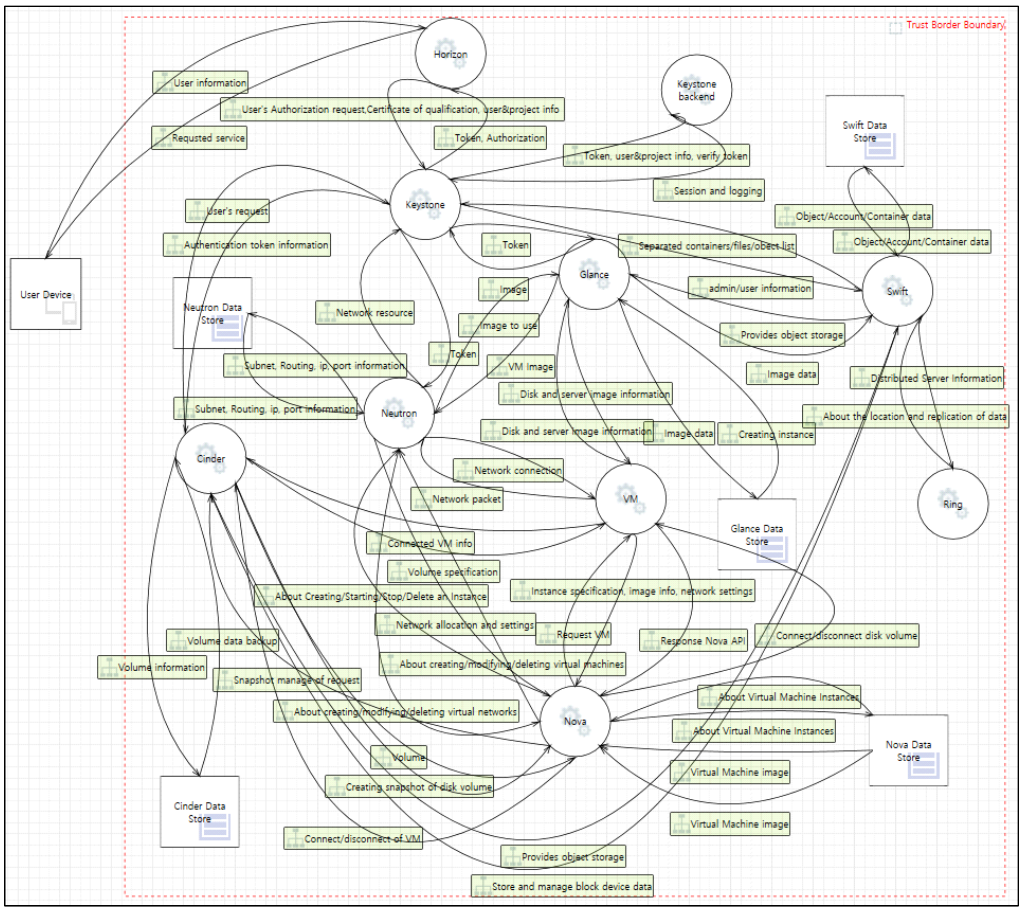

Fig. 2. Level 1 DFD

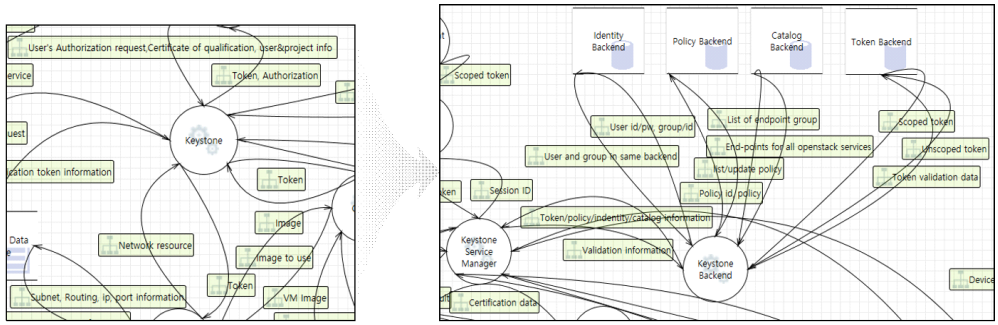

Fig. 3. Keystone DFD decomposes from Level 0 to Level 1

리하는 ▲Catalog Backend, 사용자의 임시 토큰을 관리하는 ▲Token Backend로 세분화되는 것을 Fig 3.을 통해 볼 수 있다.

▲Keystone Backend와 ▲Identity Backend 간에는 데이터는 사용자, 그룹, 프로젝트, 역할 및 인증 토큰과 같은 신원 정보와 인증 정보가 오고 가는 것을 볼 수 있다. ▲Keystone Backend는 Identity 정보와 관련된 데이터를 저장하고 Keystone 서비스의 메타데이터와 정책 설정을 관리한다. ▲Identity Backend는 사용자와 서비스에 대한 인증을 수행하고 인증 토큰을 생성하여 다른 OpenStack 서비스에 제공한다. 인증 토큰은 사용자 또는 서비스가 다른 OpenStack 서비스에 액세스할 수 있는 권한을 부여하는 데 사용된다. ▲Keystone Backend와 ▲Policy Backend 간에는 Keystone의 정책 관련 데이터가 오고 간다. ▲Policy Backend는 권한 정책 및 접근 제어를 설정하고 이를 기반으로 사용자 및 서비스에 대한 접근제어를 수행한다. ▲Keystone Backend와 ▲Catalog backend 간에는 OpenStack 서비스 엔드포인트 및 API 엔드포인트 정보가 오고 간다. ▲Keystone Backend는 OpenStack 서비스 카탈로그 정보를 저장하고 업데이트하며 ▲Catalog Backend는 사용자 및 클라이언트에게 서비스에 대한 엔드포인트 정보를 제공한다.

▲Keystone Backend와 ▲Token Backend 간에는 인증 토큰 관련 정보가 오고 간다. ▲Token Backend는 ▲Keystone에서 발급한 인증 토큰 정보를 저장하고 관리한다. 이 정보는 사용자의 인증 및 권한 부여를 확인하고 인증 토큰의 수명과 유효성을 추적한다. 이를 통해 Keystone은 사용자와 서비스에 대한 인증 및 권한 부여를 관리하고 OpenStack 서비스에 대한 접근을 허용 또는 거부한다. 이처럼 OpenStack의 Keystone은 여러 하위 모듈로 구성된다. Keystone과 하위모듈은 상호작용을 통해 사용자와 서비스에 대한 인증 및 접근권한을 부여하여 OpenStack 서비스에 대한 권한을 설정하는 것을 볼 수 있다. Level 1의 전체 데이터 흐름도는 다음 URL[1]에 제시되어 있다.

3.2 공격라이브러리 수집

공격라이브러리 수집 단계는 분석 대상과 관련된 취약점을 모두 수집하는 단계에 해당한다. 이러한 공격라이브러리는 분석 대상 시스템과 유사한 취약점 및 공격 기법을 수집하여 분석 대상 시스템에서 발생 가능한 위협을 구체적으로 식별할 수 있도록 도와준다. 공격라이브러리는 CVE(Common Vulnerabilities and Exposures), CWE(Common Weakness Enumeration), 논문, 표준 및 기술보고서 등과 같이 현재까지 알려진 취약점 관련 정보들을 수집하여 데이터베이스화 된다. 본 논문에서는 OpenStack 및 클라우드 환경과 관련된 CVE 68건, CWE 7건, 논문 32건, 컨퍼런스 4건, MITRE ATT&CK 458건으로 총 569건의 취약점을 수집하여 공격라이브러리를 구축하였다. 다음 Table 1.은 연구팀이 도출한 제로트러스트 기반의 원격 근무 환경 데이터 흐름도에 대한 공격라이브러리를 나타내며, 각 공격라이브러리의 식별자는 Attack Library의 약어인 “AL”과 해당 공격라이브러리의 출처에 대한 약어(예: CVE=“V”, Paper=“P” 등)를 수집된 순서대로 숫자를 조합하여 “AL-V-1”, “AL-P-2”와 같이 표현된다.

1) https://arxiv.org/ftp/arxiv/papers/2401/2401.03675.pdf (7page)

Table 1. Attack Library

No.	Title	Ref
AL-C-1	Attacking and Defending the Microsoft Cloud (Office 365 & Azure AD)	[32]
…		
AL-V-1	CVE-2022-47951	[33]
…		
AL-A-458	System Shutdown/Reboot	[34]

3.3 위협분석

위협분석 단계는 앞서 작성한 데이터 흐름도를 기반으로 분석 대상 시스템에서 발생할 수 있는 잠재적 위협을 식별하는 단계이다. 본 논문에서는 STRIDE 기법을 이용하여 위협을 분류하였다. STRIDE 위협 모델링 방법에는 'STRIDE per interaction'과 'STRIDE per element' 2가지 접근 방식이 존재한다. 'STRIDE per Element'는 'STRIDE per Interaction'에 비해 실제 위협에 해당하는 결과를 더 많이 도출하는 높은 정탐(true positive) 비율을 갖는다. 이에 따라 본 논문에서는 2가지의 접근방식 중 전체 구성요소에 대해 각각의 분석을 수행하는 'STRIDE per Element' 접근 방식을 사용하여 각 구성요소에 대한 위협을 총 402개 식별하였다. 식별된 위협이 실제 활용되는지 확인하기 위해 3.2에서 구축한 공격 라이브러리와의 상관관계를 Table. 2에 포함하였다.

Table 2. STRIDE between DFD elements and Attack Library

Elements	Id	Name	Threat	Attack library	No.
Entity	E1	User Device	S	AL-A-7, AL-A-20, AL-A-21, AL-A-22, AL-A-38, AL-A-39, AL-A-40, AL-A-43, AL-A-46, AL-A-59, AL-A-60, AL-A-62, AL-A-63, AL-A-64, AL-A-105, AL-W-3, AL-V-16, AL-V-17, AL-P-21, AL-A-361	T1
…					
Process	P43	Volume Backup	E	AL-V-1	T402

3.4 공격 트리 도출

공격 트리 도출 단계는 분석 대상 시스템에서 발생 가능한 위협을 이용하여 공격 시나리오를 도출하는 단계에 해당한다. 최상의 노드는 공격자의 공격 목표를 나타내며, 최하위 노드는 각 공격 시나리오를 수행하기 위한 진입점에 해당한다. 공격자가 해당 시나리오를 통해 공격을 수행하는데 필요한 시스템 내 잠재적 위협을 의미한다. 이러한 공격 트리를 통해 3.3절에서 수집된 위협들이 실제로 어떻게 공격에 사용될 수 있는지를 시각적으로 파악할 수 있다. 본 연구팀은 클라우드 환경에서 발생하는 주요 위협을 기반으로, 공격 목표를 사용자 디바이스 내 저장된 계정정보 탈취, 사용자 서비스 이용 방해, 스토리지 데이터 탈취 및 변조 총 3가지로 제시하였다. 본 연구팀은 각 공격 목표를 달성하기 위한 경로를 하위 노드로 나타내었으며, 최상위 공격노드를 통해 총 42가지의 최하위 공격목표를 식별하였다.

첫 번째 공격 트리는 사용자 디바이스 내 저장된 계정정보 탈취에 대한 공격 트리이다. 공격자는 사용자 디바이스 스니핑, 특수 패킷 전송, 네트워크 포트를 통한 접근 등을 통해 사용자 디바이스에 접근하여 권한을 획득할 수 있다. 공격자는 사용자 권한 획득 후에 기업의 내부 자산에 접근하여 디바이스 내 계정정보를 탈취할 수 있다. Fig 4.는 사용자 디바이스 내 저장된 계정정보 탈취에 대한 공격 트리를 보여준다.

두 번째 공격 트리는 OpenStack 서비스 이용 방해에 대한 공격 트리이다. 공격자는 클라우드 환경 내 구성요소들을 파괴하거나 비정상적인 트래픽을 발생시키는 등의 공격 방법을 통해 OpenStack 클라우드 서비스를 이용하지 못하도록 방해할 수 있다.

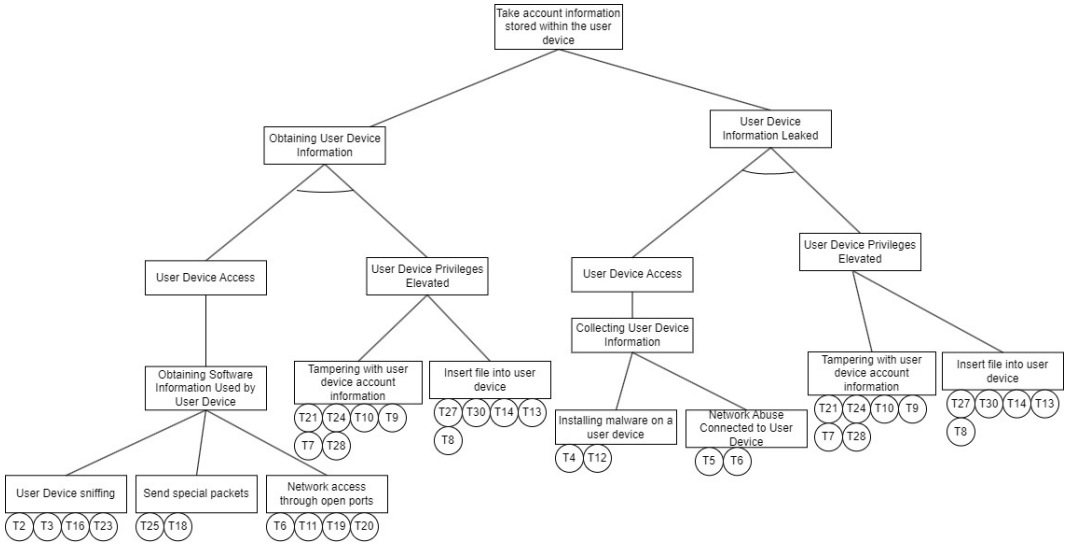

Fig. 4. Attack Tree 1

해당 공격 목표를 달성하는 것으로 공격자는 사용자가 클라우드 서비스를 정상적으로 활용하지 못하게 하여 기업의 가치를 떨어트릴 수 있다. 서비스 이용 방해에 대한 공격 트리의 경우 Horizon, Keystone, Nova Service Manager, Neutron server, Swift Proxy, Glance Service Manager, Cinder Service Manager의 이용 방해 루트노드로 이루어져 있다. OpenStack 서비스 각각의 리프노드들은 공격자가 서비스 이용 방해 공격을 수행하기 위한 공격경로를 나타낸다. 악의적인 공격자가 내부 직원의 디바이스를 감염시키고 계정정보를 탈취하여 OpenStack Cloud Horizon에 접근하여 Keystone 접근권한을 획득할 수 있다. Keystone 접근권한을 획득하면 악의적인 공격자는 인증 토큰을 발급받아 로그인에 성공하여 정상적인 사용자로 위장할 수 있게 된다. 그 후, 공격자는 대량의 API를 요청하여 더미 트래픽을 발생시켜 서비스 이용 방해 공격을 수행할 수 있다.

세 번째 공격 트리는 OpenStack Storage 데이터 탈취 및 변조에 대한 공격 트리이다. 공격자는 OpenStack Storage에 대한 관리자 권한을 획득하고 OpenStack Storage 내 데이터를 변조하여 사용자의 서비스를 방해할 수 있다. 또한, 공격자는 악성코드 배포 등을 통해 사용자 디바이스를 감염시키는 행동을 수행할 수 있다. 두 번째 공격트리와 세 번째 공격트리의 경우 URL[2]에 제시되어 있다.

3.5 보안요구사항 도출

본 연구에서는 3.4절에서 작성한 공격트리의 공격목표를 공격자가 달성할 수 없도록 공격트리의 최하위 노드인 공격방법의 대응책으로서 보안요구사항을 총 80개 도출하였다. OpenStack에서는 자사의 클라우드 서비스에 대한 보안 체크리스트[35] 총 45개를 제공하고 있다. 해당 체크리스트에서는 파일 권한 설정, TLS 활성화 등과 같은 항목을 다루고 있지만 제로트러스트 원칙이 적용되었다고 보기 어렵다. 또한 해당 체크리스트가 존재하더라도 지속적으로 취약점이 발견되고 있다[36-41]. 또한, 기존 제로트러스트 기반 보안요구사항을 도출하는 학술 연구들은 클라우드 시스템의 전체 서비스가 아닌 특정 상황 및 특정 모듈에 한정되어 있었다. 하지만 본 연구팀은 클라우드 전반적인 시스템을 다루는 보안요구사항을 도출하였다. 본 연구에서는 클라우드 서비스를 이루고 있는 핵심 구성요소 별로 도출하였기 때문에 NIST 및 DoD보다 구체적이고 더 많은 보안요구사항을 도출하였다. 도출된 보안요구사항은 제로트러스트 원칙을 준수하며 이를 기반으로 세분화 되어 크게 '지속적 인증을 통한 접근제어', '네트워크 암호화 및 세그먼테이션', '지속적인 모니터링' 등으로 구성된다. 본 연구팀이 도출한 보안요구사항은 제로트러스트 7

2) https://arxiv.org/ftp/arxiv/papers/2401/2401.03675.pdf (10-11page)

Table 3. Security Requirements

Attack/Threat	Location	Security Requirements
User Device Sniffing	User Device	Moving beyond existing firewalls based on ports and protocols, abnormal packets must be detected and filtered using next-generation firewalls (NGFWs) based on user ID, application recognition, and context awareness functions. a) Analyze connection status, protocol header, source and destination IP, source and destination port number, TCP status, ongoing application, and if malicious packets are detected, block and record the traffic. b) Utilizes iptables to block packets in transit until communication is authenticated and approved by the policy engine c) For ongoing applications, identify the application using payload size analysis, session request/response count analysis, and dynamic/regular expression pattern searching within packets. d) In the case of packet encryption, Segmentation and Encapsulation is applied to segment network packets to encrypt and encapsulate each packet so that data is additionally encrypted at each step in the entire communication.
...		

원칙에 모두 매핑되며 NIST 및 DoD의 보안요구사항과 NIST 정보시스템 관련 표준[21], 여러 학술연구를 기반으로 구체화되었다. 일반적으로 인증, 마이크로 세그멘테이션, 트래픽 암호화와 같은 요구사항이 클라우드의 전체적인 구성요소에 필요한 것으로 파악되었다. 또한, 인증 서버와 같은 클라우드 서비스를 위한 주요 구성요소의 경우 가용성 유지와 같은 요구사항도 필요한 것으로 파악되었다. 클라우드 서비스 제공자는 상세한 보안요구사항을 통해 클라우드 기반 원격 근무 환경의 보안정책을 설계하고 구현할 수 있다. 이는 시스템 내 무단접근, 데이터 유출, 악성 코드 감염 등과 같은 위협에 대비할 수 있도록 도와준다. 또한, 상세한 보안요구사항은 보안위협을 식별하고 관리하는데 도움이 된다. 이를 통해 잠재적인 위협에 대한 예방 및 대응 전략을 수립할 수 있다. 마지막으로, 상세한 보안요구사항은 시스템 내 발생하는 보안 이슈에 대해 신속하게 대응할 수 있도록 도와준다. 보안이슈가 발생했을 때 효과적으로 대응할 수 있는 기술을 사전에 마련할 수 있기 때문이다. 이처럼 상세한 보안요구사항을 도출함으로써 전반적인 원격 근무 환경에서의 보안을 강화하고 발생 가능한 보안 위협을 대응 및 예방하여 피해를 최소화할 수 있다. 이에 따라 본 연구팀은 Table. 3과 같이 총 80개의 상세한 보안요구사항을 도출하였다. 전체 보안요구사항은 다음 URL[3]에 제시되어 있다.

Table 4.는 ABAC 관련 보안요구사항에 해당하는 예시에 해당한다. 해당 예시를 통해 본 논문에서 도출한 보안요구사항이 NIST 및 DoD의 보안요구사항에 비해 어떻게 상세화 및 차별화되는지를 나타낸다. NIST 및 DoD에서 발간한 제로트러스트 아키텍처 표준이 존재하지만 구체적인 기술 적용 방법에 대해서는 클라우드 서비스 제공자마다 해석이 분분하다. NIST 및 DoD의 ABAC 관련 보안요구사항의 경우, 개체에 할당된 속성 값에 따라 접근을 제어해야 한다고만 서술되어 있다. 이는 어떠한 속성 값, 절차 등을 통해 접근제어를 수행하는지에 대해 서술되어 있지 않아 클라우드 서비스 제공자의 입장에서 해당 보안요구사항에 대한 설명이 불충분할 수 있다. 즉, 설명이 불충분한 보안요구사항은 클라우드 서비스 제공자에게 심층적인 이해를 제공하지 않아 제로트러스트 기반 클라우드 환경을 구축할 때, 이해관계자 간의 혼란을 야기할 수 있다. 추상적으로 기술된 보안요구사항 중 유사한 내용을 포함하는 항목이 존재하면 클라우드 서비스 제공자는 어떤 보안요구사항을 구현해야 하는지 명확히 결정할 수 없다. 그러므로, 클라우드 서비스 제공자는 상세하고 명확한 보안요구사항을 통해 안전한 원격 근무 환경을 구현할 필요가 있다. 본 연구팀은 보안요구사항을 세부 구현기능 단위로 상세화하였다. 본 연구팀이 상세화한 보안요구사항에는 어떠한 속성을 어디에 어떻게 적용해야

3) https://arxiv.org/ftp/arxiv/papers/2401/2401.03675.pdf (14-53page)

Table 4. NIST, DoD and Ours Requirement Example about ABAC

ID	Requirements
NIST ABAC	Use Enhanced Identity Governance to requests to a policy engine service or authenticate the subject and approve the request before granting access. For this approach, enterprise resource access policies are based on **identity and assigned attributes**. The primary requirement for resource access is based on the access privileges granted to the given subject.
DoD ABAC	Access should be controlled by authorizing based on the **assigned attributes of the object**, the assigned attributes of the object, environmental conditions, and a set of policies specified according to those attributes and conditions.
Ours ABAC	Access control should be performed using attribute information (user attributes, device information, location information) through an attribute-based access control model called ABAC. a) To apply ABAC, first define the attributes to control access to resources: **user roles, departments, projects, locations, and other attributes of the Keystone include entity name, domain_id, parent_id, password, project id, enabled_service, etc.).** b) **Define access rules and policies** for each resource and service (ex, define policies that only users with "department" attributes "development team" and "role" is "admin"). c) Use Keystone's policy **engine to match attributes with policies to handle actual access requests.** Keystone's **policy engine determines whether a user or group is accessible based on the attributes.** d) Modifies the "Policy configuration file" within Keystone to **enable ABAC policies and set the attributes and policies to use.** ABAC policies that allow ABAC policies to be added or changed should be tested and verified for working properly. Attempt access control with attributes and policies using Keystone API, and verify that it works as expected. e) **Implement audit and monitoring of access rules assessment and execution of ABAC systems** to detect and respond to anomalies and implement automation for management and update of ABAC rules to automatically enforce rules if required.

하는지 구체적으로 서술되며 ABAC을 적용하기 위한 절차가 세부적으로 제시되어 있다. 클라우드 서비스 제공자 및 사용자는 상세화된 보안요구사항을 준수함으로써 원격 근무 환경에서 기업 내 자산을 더욱 안전하게 유지할 수 있을 것으로 판단된다.

IV. 기존 상용 클라우드 서비스 보안성 분석

4장에서는 본 연구팀이 도출한 보안요구사항의 적합성 및 우수성을 확인하기 위해 NIST, DoD, 본 연구팀이 도출한 보안요구사항을 기반으로 제로트러스트가 적용된 클라우드 서비스에 대한 보안성 분석 결과를 서술한다. 제로트러스트가 적용된 클라우드 서비스는 클라우드 시장 내에서 점유율이 높은 Microsoft Azure, Amazon Web Service(AWS), Google Cloud로 선정하였다[42]. 본 연구팀은 Microsoft Azure[43], Amazon Web Service[44], Google Cloud[45]의 기술문서 및 가이드라인을 참조하고 실제 클라우드 서비스를 사용해봄으로써 상기 3종 클라우드 서비스에 대한 기능을 각각 158건, 247건, 146건 식별하였다. 이후 4.1절에서는 Microsoft Azure, Amazon Web Service, Google Cloud가 NIST, DoD 그리고 본 연구팀이 도출한 보안요구사항을 만족하는지 확인하였다.

4.1 보안성 분석에 대한 결과

상기 3.5절에서 언급했듯이, 본 연구팀이 도출한 보안요구사항은 제로트러스트 기반의 보안요구사항이다. 클라우드 서비스에 대한 보안성 분석을 수행하기 위해서 Microsoft Azure, Amazon Web Service, Google Cloud가 제로트러스트 기반 클라우드 서비스인지 확인하였다. 확인 결과, 각 클라우드 서비스는 NIST에서 명시하고 있는 제로트러스트 7원칙에 모두 부합하는 것으로 나타났다. 이는 Microsoft Azure, Amazon Web Service, Google Cloud가 제로트러스트 기반 클라우드 서비스임을 의미한다. 이에 따라 각 서비스 별로 NIST,

DoD, 본 연구팀이 도출한 보안요구사항 기반의 보안성 분석을 수행하였다. 보안성 분석을 수행하기 전 본 연구팀은 NIST SP 800-207과 DoD Zero Trust Reference Architecture의 보안요구사항을 각각 25개, 52개 식별하였다. NIST SP 800-207의 경우, 제로트러스트를 구현하기 위한 전략과 네트워크 요구사항 내용을 담고 있는 3장 '제로트러스트 아키텍처의 논리 컴포넌트'를 기반으로 식별하였다[6]. DoD Zero Trust Reference Architecture의 경우, 제로트러스트를 구현하기 위해 필요한 기술 및 기능을 서술하고 있는 3장 '기능분류체계'를 기반으로 식별하였다[7].

보안성 분석은 각 클라우드 서비스의 기술문서 및 가이드라인과 실제 서비스 기능 분석을 통해 수행되었다. 보안성 분석 결과는 보안요구사항을 모두 만족할 경우 "●", 일부만 만족할 경우 "◑", 만족하지 못할 경우 "-"로 표기하였다. 보안성 분석 결과, Microsoft Azure, Amazon Web Service, Google Cloud는 NIST의 요구사항 총 25개와 DoD의 요구사항 총 52개를 모두 만족하는 것으로 확인되었다. 그러나 보안성 분석 결과, 각 클라우드 서비스는 본 연구팀이 도출한 보안요구사항 중 일부 항목을 만족하지 못하였다. 이는 NIST 및 DoD의 보안요구사항을 모두 만족하더라도 잔존하는 위협이 다수 존재함을 의미한다. 또한, 3.5절에서 설명한 것과 같이 기존의 NIST 및 DoD의 보안요구사항은 많은 기업들이 따르는 가이드라인의 특성상 설명이 불충분하다는 문제점이 있다. 클라우드 서비스 제공자 및 사용자는 불충분한 보안요구사항으로 인해 보안요구사항을 올바르게 이해하지 못할 수 있다. 이는 민감한 정보의 유출, 해킹, 데이터 손상 및 다른 보안 위험을 증가시킬 수 있다. 다음 Table 5.는 Microsoft Azure, Amazon Web Service, Google Cloud에 대한 보안성 분석 결과를 간략하게 나타낸다.

Table 5. Result of Security Anaylsis

Cloud Service	NIST	DoD	Ours
Microsoft Azure	●	●	◑
Amazon Web Service	●	●	◑
Google Cloud	●	●	◑

본 연구팀이 각 클라우드 서비스의 기술문서 및 사용자 가이드라인과 실제 클라우드 서비스를 분석한 결과, Microsoft Azure는 본 연구팀이 도출한 보안요구사항 80개 중 76개를 만족하고 4개를 만족하지 못함을 확인하였다. Amazon Web Service는 본 연구팀이 도출한 보안요구사항 80개 중 76개를 만족하고 4개를 만족하지 못하였다. Google Cloud는 본 연구팀이 도출한 보안요구사항 80개 중 75개를 만족하고 5개를 만족하지 못하였다. 세 가지 클라우드 서비스가 공통적으로 만족하지 못하는 요구사항은 클라우드 환경 최초 접근 시 비밀번호 강제 변경(Ours-Secu-008), 인증서 폐기 절차(Ours-Secu-032), 주기적인 접근권한 검토(Ours-Secu-074)이다. Table 6.은 본 연구팀이 도출한 보안요구사항 중 Microsoft Azure, Amazon Web Service, Google Cloud가 공통적으로 만족하지 못하는 항목을 나타낸다.

Table 6. Ours Requirements with Microsoft Azure, Amazon Web Service, Google Cloud

ID	Ours Requirements
Ours-Secu-008	The requirements of password management procedures should be applied when designing the system. … **e) Forced change of password at first access to information system,** masking at the time of password processing (input, change).
…	…
Ours-Secu-032	A certificate disposal procedure should be established to prevent leakage of critical information stored in the Nova-cert/object store. **a) Request and confirmation of certificate retirement: Send a certificate retirement request to the SSL/TLS certificate issuing authority. At this time, the private key of the certificate and the reason for discarding the certificate must be provided together.** … **g) Record the reason for certificate disposal and information: Record the reason for certificate disposal and detailed information so that it can be verified later if necessary.**

ID	Ours Requirements
	...
Ours-Secu-074	In order to manage access to cloud systems and important information, the appropriateness of access rights, use (long-term use), and changes (retirement and leave of absence, job change, department change) should be regularly checked. Periodic review should be conducted to ensure that the allocated account and access rights are appropriate. **a) Establishment of review criteria and policies: Define criteria and policies for reviewing access rights Clarify which rights should be reviewed under what conditions and which users or roles should be reviewed.** ... **c)Determining review cycles: Periodic review cycles can be set monthly, quarterly, etc., determined by system importance and resources** **d) Selection of review targets: Selection of review targets. Priority selection of rights of high importance or sensitivity, etc.** **e) Select a review method and tool: Select the method and tool to perform the review. Use manual reviews, automated scripts, security information, and event management systems to conduct reviews.** ...

4.2 상용 시스템의 잠재 위협 및 완화방안

보안성 분석 결과, Microsoft Azure, Amazon Web Service, Google Cloud의 미흡한 부분은 클라우드 환경 최초 접근 시 비밀번호 강제 변경(Ours-Secu-008), 인증서 폐기 절차(Ours-Secu-032), 주기적인 접근권한 검토(Ours-Secu-074)이다.

클라우드 환경 최초 접근 시 비밀번호 강제 변경(Ours-Secu-008) 관련 보안요구사항에는 클라우드 환경 최초 접근 시 비밀번호를 강제로 변경해야 한다고 명시되어 있다. 각 클라우드 서비스에는 최초 로그인 시 본인인증, 비밀번호 만료 기간 설정 등을 비롯한 비밀번호 정책이 존재한다. 하지만 클라우드 서비스 사용자가 클라우드 환경에 최초 접근할 때 사용자가 회원가입 시 설정한 비밀번호 그대로 로그인이 가능하기 때문에 해당 보안요구사항을 만족한다고 보기 어렵다. 클라우드 서비스 사용자가 클라우드 환경에 최초 접근할 때 사용자의 비밀번호를 강제로 변경하지 않으면, 악의적인 공격자가 사용자 계정을 통해 무단으로 클라우드 환경에 접속하여 악성 소프트웨어의 설치, 데이터 변조 등과 같은 활동이 이루어질 수 있다. 공격자의 계정탈취를 통해 클라우드 서비스에 접근하게 되는 경우 중요 데이터를 탈취하거나 서비스를 중단시키는 등의 보안사고가 발생할 수 있다. IBM 조사에서도 우리나라 데이터 유출사고의 20%가 사용자 인증정보를 이용해 최초 침투한 것으로 나타났다[46].

인증서 폐기 절차(Ours-Secu-032) 관련 보안요구사항에는 클라우드 서비스 사용자가 인증서 폐기를 요청할 때 클라우드 서비스 사용자로부터 폐기 이유를 함께 제공받아야 하며, 이에 대한 기록 및 문서화가 이루어져야 한다고 명시되어 있다. 각 클라우드 서비스는 인증서 생성 및 폐기 기능을 제공하지만, 클라우드 서비스 사용자에게 인증서 폐기 이유를 요구하지 않는다. 그리고, 각 클라우드 서비스에서 사용자는 인증서 삭제 버튼을 누르면 바로 영구적으로 인증서를 삭제할 수 있다. 따라서, 각 클라우드 서비스는 인증서를 폐기하는 이유에 대한 기록을 수행하고 문서화하는 기능을 제공한다고 보기 어렵다. 공격에 많이 사용되는 피싱은 위조된 웹사이트를 통해 사용자의 계정정보와 개인정보를 탈취한다. 피싱 사이트에도 SSL/TLS 인증서가 적용돼 있어 인증서 유무만으로 피싱 사이트인지 아닌지 분별하기 어렵다. 그러므로 피싱사이트의 경우 빠르게 제작되는 만큼 인증서 관리가 중요하다. HTTPS 웹사이트가 증가함에 따라 SSL/TLS 인증서는 온라인 통신을 보호한다. 따라서 SSL 인증서의 개인 키가 손상되면 엔드투엔드 암호화의 안전한 통신 보증이 위협받을 수 있다. 보안업체 멘로 시큐리티(menlo security)의 CTO인 코우식 구루스와미(kowsik guruswamy)는 최근 HTTPS 웹사이트들을 조사한 결과 47.1%에서 취약한 서버 소프트웨어, 오래된 아파치(apache), 드루팔(drupal), 워드프레스(wordPress)가 발견되었다고 말한다. 브라우저가 아닌 다른 곳에서 발생하는 트래픽의 67%는 SSL로부터 발현하는 것으로 나타났다. 구루스와미는 피싱 링크나 드라이브 바이 다운로드를 SSL에 호스팅 하면 아무도 검사하지 않기 때

문에 공격을 쉽게 성공시킬 수 있다고 말한다.[47]. 인증서 폐기 이유를 기록하지 않으면 보안 이슈나 침해 사고가 발생했을 때, 이를 추적하기가 어렵다.

주기적인 접근권한 검토(Ours-Secu-074) 관련 보안요구사항에는 클라우드 서비스 사용자의 계정 및 접근권한이 적절한지에 대해 주기적인 검토가 수행해야 되어야 한다고 명시되어 있다. 각 클라우드 서비스는

RBAC 또는 ABAC을 통한 접근권한 제어를 수행한다. 하지만, 접근권한에 대한 검토를 주기적으로 수행하는 기능은 존재하지 않아 해당 보안요구사항을 만족한다고 보기 어렵다. 주기적인 접근권한 검토가 이루어지지 않으면 사용자가 현재 불필요한 권한을 계속 보유할 수 있다. 팔로알토 네트웍스에 따르면 분석 결과 클라우드 사용자, 역할, 서비스 및 리소스의 99%에 60일 동안 사용하지 않은 '과잉 권한'이 부여된 것으로 나타났다[48]. 해당 보고서에서는 해커가 이러한 권한을 악용하여 공격 반경을 횡적, 종적으로 모두 확장할 수 있다고 경고하고 있다. 또한, 불충분한 접근관리로 인해 정상적인 사용자로 가장한 악의적인 행위자는 전송중인 데이터 읽기, 수정, 삭제 등이 가능하다. 즉, 데이터에 무단으로 액세스 할 수 있으며 기업 또는 조직의 중요 정보를 외부에 유출할 수 있다. Azure, AWS, Google Cloud가 만족하지 못하는 보안요구사항은 기능적 측면도 존재하나 접근 권한 검토 관련 보안요구사항처럼 조직적 차원 즉, 사용자가 준수해야 하는 보안요구사항에 해당하는 부분도 존재한다. 이에 따라 제로트러스트 기반 안전한 원격 근무 환경을 구축하기 위해서는 Azure, AWS, Google Cloud의 기능적 측면도 고려되어야 하지만 사용자의 보안 교육도 고려되어야 하는 것으로 나타났다. Table 7.은 본 연구팀이 도출한 보안요구사항들 중 Azure, AWS, Google Cloud에서 공통적으로 만족하지 못한 항목을 나타내며, 이로 인해 발생할 수 있는 보안 위협과 완화방안에 대한 표에 해당한다.

4.2.1 Microsoft Azure의 잠재 위협 및 완화방안

Microsoft Azure는 상기 4.1~4.2절에서 기술한 보안요구사항 외에 가상환경 수립 시 출처가 명확한 소프트웨어 설치(Ours-Secu-035) 관련 보안요구사항이 미흡하다. Microsoft Azure의 경우 주기적인 보안 업데이트 및 악성 소프트웨어를 감지하고 차단하기 위한 모니터링 기능 등은 존재하나, 클라우드 사용자들에게 출처가 명확한 소프트웨어만 설치할 것을 권장하는 정책과 가이드라인은 제시하지 않는다. 출처가 명확한 소프트웨어를 사용하도록 권장하는 정책 및 가이드라인이 없는 경우 클라우드 서비스 사용자들은 안전하지 않은 소프트웨어를 설치할 가능성이 높아진다. 정상 파일로 위장해 설치를 유도하는 이 공격은 많은 소프트웨어 사용 기업을 감염시킬 수 있다. 최근 북한의 해킹그룹 안다리엘(andariel)이 특정 자산관리 프로그램을 이용한 공격을 통해 악성코드를 유포하는 공격이 발생하고 있다[49]. 초기 침투 시 주로 스피어피싱 공격이나 워터링 홀 공격, 그리고 소프트웨어의 취약점을 이용하는 것으로 알려져 있다. 또한, 공격 과정에서 다른 취약점을 이용해 악성코드를 배포하는 정황도 확인되고 있다. 이에 사용

Table 7. Common possible security threats and countermeasures

No.	Ours Requirements	Security Threats	Countermeasures
Ours-Secu-008	Forced change of password on first access to information systems.	- Malicious activity - Misuse of authority - Failure to comply with the latest security policies	Provide random passwords to users when accessing information systems for the first time
Ours-Secu-032	Record the reason for the certificate disposal and detailed information so that it can be verified later if necessary.	- Forgery of certification - Data integrity issues - Difficulty in detecting security incidents	Document the reasons for discarding the certificate and its contents when discard certificate
Ours-Secu-074	Periodic review should be conducted to ensure that the allocated account and access control are appropriate.	- Authorization Error - Data leakage - Increased likelihood of abuse	Periodically conducting reviews of permissions at the organization level
...			

Table 8. Possible security threats and countermeasures of Microsoft Azure

No.	Ours Requirements	Security Threats	Countermeasures
Ours-Secu-035	Establish policies and guidelines that encourage cloud users to install only software with a clear source	- Installing Malicious Software - Security attributes such as confidentiality, integrity, and availability are threatened	Organizations should establish policies and guidelines that encourage cloud users to install only software with a clear source.

자들은 출처가 불분명한 파일 및 소프트웨어를 각별히 주의해야한다. 이로 인해 시스템 내 자산의 기밀성, 무결성, 가용성이 훼손될 수 있기 때문이다. 이에 따라 조직은 적절한 가상환경의 소프트웨어 설치에 대한 교육을 수행하고 기업 내부에서 관련 정책 및 가이드라인을 수립해야 한다. Table 8.은 Microsoft Azure에서 발생 가능한 잠재 위협과 이를 완화하기 위한 방안을 나타낸다.

4.2.2 Amazon Web Service의 잠재 위협 및 완화방안

Amazon Web Service는 상기 4.1~4.2절에서 기술한 보안요구사항 외에 가상환경 설정에 대한 사용자 교육(Ours-Secu-062) 관련 보안요구사항이 미흡하다. AWS는 자사 클라우드의 다양한 기능에 대한 사용자 교육 및 사용자 가이드라인을 제공하고 있지만 인스턴스의 저장 공간에 대한 사용자 교육(Ours-Secu-062)과 관련된 기능은 존재하지 않는다. 해당 보안요구사항을 준수하지 않을 경우 사용자가 인스턴스나 저장 공간을 적절히 관리하지 못하면 비효율적인 리소스 사용이 발생할 수 있다. 사용자가 인스턴스나 저장 공간을 과도하게 사용하면 리소스가 고갈되어 정상적인 서비스 이용이 어려워진다. 공격자는 공격 대상 클라우드 서비스가 프로세서, 메모리, 디스크 공간, 또는 네트워크 대역폭과 같은 한정된 시스템 리소스를 과도하게 소비하도록 해 시스템 속도를 저하시키고 정상적인 서비스 사용자가 서비스에 접근할 수 없도록 만든다. 버라이즌 DBIR(Data Breach Investigations Report)에 따르면, 디도스 공격은 전체 사이버 보안 위협의 46%를 차지하면서 가장 큰 위협으로 꼽히고 있으며 증가 추세 역시 높은 수준인 것으로 나타났다[50]. 그러므로 기업 내 클라우드 서비스 사용자들에게 적절한 교육 및 훈련이 제공되어야 한다. 또한 클라우드 서비스 사용자들은 인스턴스의 저장공간과 가상머신 관련 작업에 대한 정책 및 보안 규칙을 명확하게 수립해야 한다. Table 9.는 Amazon Web Service에서 발생 가능한 잠재 위협과 이를 완화하기 위한 방안을 나타낸다.

4.2.3 Google Cloud의 잠재 위협 및 완화방안

Google Cloud는 상기 4.1~4.2절에서 기술한 보안요구사항 외에 가상환경 설정에 대한 사용자 교육(Ours-Secu-062), 이미지 유효성 검증(Ours-Secu-077) 관련 보안요구사항이 미흡하다. 상기 4.2.2.절에서 설명한 바와 같이 가상환경 설정에 대한 사용자 교육 관련 요구사항은 조직적 차원에서 준수해야 하는 요구사항에 해당한다. 해당 보안요구사항을 준수하지 않음으로써 발생할 수 있는 위협은 상기 4.2.2절과 동일하다. Google Cloud는 클라우드 서비스 사용자가 이미지를 생성할 때 이미지가 지원하지 않는 포맷인 경우 해당 이미지가 생성되지 않지만, 이미지의 유효성을 검사하는 항목은 존재하지 않는다. 공격자는 이미지를 통해 시스템에 악성코드를 삽입하여 시스템을 감염시킬 수 있다. 또한,

Table 9. Possible security threats and countermeasures of Amazon Web Service

No.	Ours Requirements	Security Threats	Countermeasures
Ours-Secu-062	Educate users and enhance their awareness of virtual environments	- Performance degradation due to inefficient resource use - Denial of Service Attack (DoS)	Recognize and educate users about policies and security rules for instance and storage-related tasks

Table 10. Possible security threats and countermeasures of Google Cloud

No.	Ours Requirements	Security Threats	Countermeasures
Ours-Secu-062	Educate users and enhance their awareness of virtual environments	- Performance degradation due to inefficient resource use - Denial of Service Attack (DoS)	Recognize and educate users about policies and security rules for instance and storage-related tasks
Ours-Secu-077	Validate an image and verify that it is from a trusted source	- Inserting malicious code - Tampering image - Vulnerability Exploits	Validates images when using them in a cloud environment, establishes and complies with policies to use only trusted images

검증되지 않은 이미지는 중간에서 변조될 가능성이 존재하며 공격자가 이미지를 통해 시스템의 취약점을 이용하여 공격을 수행할 수 있다. 해커그룹 TeamTNT는 새로운 도커 허브(docker hub) 계정을 만들어 악성 도커 이미지(docker image)들을 업로드했다. 이들은 도커 허브에 정상으로 위장한 악성 도커 이미지들을 업로드해 악성코드를 배포하였다[51]. 이러한 보안 위협을 방지하고 최소화하기 위해서는 클라우드 환경에서 이미지를 사용할 때 유효성을 검증해야 한다. 또한, 기업 내 조직은 신뢰할 수 있는 이미지만을 사용하도록 정책을 수립하고 클라우드 사용자는 해당 정책을 준수하도록 해야한다. Table 10.은 Google Cloud에서 발생 가능한 잠재 위협과 이를 완화하기 위한 방안을 나타낸다.

V. 결 론

본 연구팀은 제로트러스트 기반의 원격 근무 환경을 구축하기 위한 보안요구사항 분석 연구를 수행하였다. 기존의 NIST 및 DoD의 보안요구사항은 추상적으로 작성되어 있어 서비스 제공자가 구체적인 취약점을 식별하고 완화하기 어렵다. 이로 인해 서비스 제공자가 보안 위협에 대응하는데 어려움이 발생할 수 있다. 이 외에도 원격 근무 환경에서 식별되지 않은 취약점이 존재할 경우, 데이터 유출, 무단 액세스 등과 같은 보안 문제가 발생할 수 있다. 이에 따라, 본 연구팀은 상세한 보안요구사항을 도출하기 위해 OpenStack을 대상으로 위협모델링을 수행하였다. 위협모델링 수행 결과, 총 80개의 보안요구사항이 도출되었으며, 제로트러스트 원칙이 적용된 상용 클라우드 서비스 3종을 대상으로 보안성 분석이 진행되었다. 본 연구팀이 보안성 분석을 수행한 결과, Microsoft Azure, Amazon Web Service, Google Cloud는 기존의 NIST 및 DoD의 보안요구사항은 모두 만족하는 것을 확인하였다. 그러나, Microsoft Azure, Amazon Web Service, Google Cloud는 본 연구팀이 도출한 보안요구사항의 세부 항목들에 대해서는 일부 만족하지 못했다. 이와 같은 결과는 원격 근무 환경 내에서 공격자의 악성 행위, 권한 오용, 데이터 유출 등과 같은 문제가 발생할 수 있음을 의미한다. 따라서 클라우드 서비스 제공자는 본 논문에서 제시한 보안요구사항을 통해 데이터 암호화, 네트워크 보안, 가상환경 보안 등 보다 세부적인 지침을 통해 다양한 보안 기술을 구현하고 관리할 수 있다.

보안성 분석 결과 클라우드 서비스 제공자뿐만 아니라 클라우드 사용자의 역할 또한 중요하다. 이에 따라 클라우드 사용자가 보안관련 정책과 기술을 활용할 수 있도록 사용자의 고려사항을 도출하는 연구가 추후 수행되어야 한다. 조직 내 자체적인 보안정책을 수립하고 클라우드 서비스 제공자가 제공하는 다양한 보안 기능을 활용하여 자체 시스템의 안전성을 유지하며 클라우드 서비스를 안전하게 관리할 수 있기 때문이다. 이러한 점을 고려할 때, 본 논문에서 제안하는 상세한 보안요구사항을 활용한다면 보다 안전한 제로트러스트 기반의 원격 근무 환경에 대한 설계 및 개발이 가능할 것으로 판단된다.

References

[1] Satya Nadella, "Microsoft Build 2020: CEO Satya Nadella's opening remarks",

https://www.youtube.com/watch?v=S_wNRx7f7rU, May. 2020.
〔2〕 Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023", https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023, Apr. 2023.
〔3〕 Trend Micro, Trend Micro Research, "A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report", Trend Micro Research, Feb. 2021.
〔4〕 Microsoft, "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction By Microsoft Incident Response", https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction, Sep 2023.
〔5〕 John Kindervag, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security", Forrester, Sep. 2010.
〔6〕 National Institute of Standards and Technology, "NIST SP 800-207 Zero Trust Architecture", Aug. 2020.
〔7〕 Defense Information Systems Agency (DISA) And National Security Agency (NSA) Zero Trust Engineering Team, "Department Of Defense Zero Trust Reference Architecture, Version 2.0", Jul. 2022.
〔8〕 Forrester, "The I&O Pro's Guide to Enterprise Open Source Cloud Adoption, Q1 2018", Mar. 2018.
〔9〕 Ward, Rory, and Betsy Beyer, "Beyondcorp - A New Approach To Enterprise Secuirty", Google, Dec. 2014.
〔10〕 Gartner, "The Gartner IT Security Approach for the Digital Age", https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age, Sep. 2023.
〔11〕 Bryan Zimmer, "LISA: A Practical Zero Trust Architecture", Usenix, Jan. 2018.
〔12〕 Theo Dimitrakos, Tezcan Dilshener, Alexander Kravtsov, Antonio La Marra,Fabio Martinelli, Athanasios Rizos, Alessandro Rosetti and Andrea Saracino, "Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1801-1812, Dec. 2020.
〔13〕 Mandal, S., Khan, D.A. and Jain, S., "Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic", New Gener. Computing. vol. 39, pp. 599–622, 2021.
〔14〕 P. García-Teodoro, J. Camacho, G. Maciá-Fernández, J.A. Gómez-Hernández and V.J. López-Marín, "A novel zero-trust network access control scheme based on the security profile of devices and users", Computer Networks, vol. 212, article. 109068, May. 2022.
〔15〕 Nisha T N, Dhanya Pramod and Ravi Singh, "Zero trust security model: Defining new boundaries to organizational network", Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing, pp. 603-609, Aug. 2023.
〔16〕 ACT-IAC, "Zero Trust Report - Lessons Learned From Vendor And Partner Research", May. 2021.
〔17〕 Alper Kerman, Oliver Borche, Oliver

Borche, Eileen Division and Allen Tan, "IMPLEMENTING A ZERO TRUST ARCHITECTURE", NCCoE, Oct. 2020.
[18] DISA and NSA, "Department of Defense (DOD) Zero Trust Reference Architecture Version 1.0", Feb. 2021.
[19] NSA, "Embracing A Zero Trust Security Model", Feb. 2021.
[20] CISA, "Zero Trust Maturity Model", Apr. 2023.
[21] National Institute of Standards and Technology, "NIST SP 800-53 Security and Privacy Controlsfor Information Systems and Organizations", Sep. 2020.
[22] Microsoft, "Zero Trust security", https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust, Jun. 2023.
[23] Microsoft, "Evolving Zero Trust - How Real-World Deployments And Attacks Are Shaping The Future Of Zero Trust Strategies", Sep. 2021.
[24] AWS, "Understanding Zero Trust principles", https://docs.aws.amazon.com/us_en/prescriptive-guidance/latest/strategy-zero-trust-architecture/zero-trust-principles.html, May. 2023.
[25] Google, "Google Cloud Architecture Framework", https://cloud.google.com/architecture/framework, Google Cloud, Jun. 2023.
[26] Victor Escobedo, Betsy Beyer, Max Saltonstall and Filip Żyźniewski, Google, "Beyondcorp 5 - The User Experience", Sep. 2017.
[27] R. Khan, K. McLaughlin, D. Laverty and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems", 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1-6, Sep. 2017.
[28] M. Cagnazzo, M. Hertlein, T. Holz and N. Pohlmann, "Threat modeling for mobile health systems", 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 314-319, Apr. 2018.
[29] Zaina Abuabed, Ahmad Alsadeh and Adel Taweel, "STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles", Computers & Security, Computers & Security, vol. 133, article. 103391, Oct. 2023.
[30] Microsoft, "Microsoft Threat Modeling Tool", https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool, Aug. 2022.
[31] OpenStack, "OpenStack documentation-design", https://docs.openstack.org/arch-design/design.html, May. 2023.
[32] Sean Metcalf and Mark Morowczynski, "Attacking and Defending the Microsoft Cloud (Office 365 & Azure AD)", Black Hat USA, Aug. 2019.
[33] MITRE CVE, "CVE-2022-47951", https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-47951, Feb. 2023.
[34] The MITRE Corporation, https://attack.mitre.org/techniques/T1529, May. 2023.
[35] OpenStack, "OpenStack documentation-security checklist", https://docs.OpenStack.org/security-guide/checklist.html, Jan. 2023. May. 2023.
[36] MITRE CVE, "CVE-2023-40585", https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40585, May. 2023.
[37] MITRE CVE, "CVE-2023-3637", https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3637, Jul. 2023.
[38] MITRE CVE, "CVE-2023-2088", https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2088, Jul. 2023.
[39] MITRE CVE, "CVE-2023-1636", https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1636, Apr. 2023.
[40] MITRE CVE, "CVE-2023-1633", https://

cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1633, Mar. 2023.
〔41〕 MITRE CVE, "CVE-2023-1625", https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1625, Mar. 2023.
〔42〕 Synergy Research Group, "Huge Cloud Market Still Growing at 34% Per Year; Amazon, Microsoft & Google Now Account for 65% of the Total", https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues, Apr. 2023.
〔43〕 Microsoft, "Azure documentation", https://learn.microsoft.com/en-us/azure/?product=popular, Jun. 2023.
〔44〕 AWS, "Welcome to AWS Documentation", https://docs.aws.amazon.com, Jun. 2023.
〔45〕 Google Cloud, "Google Cloud Document ation", https://cloud.google.com/docs?hl=us, Jun. 2023.
〔46〕 IBM Security, Cost of a Data Breach Report 2021, Aug 2021.
〔47〕 Menlo Security, "The Critical Role of SSL Decryption & Inspection in Web Security", https://www.menlosecurity.com/blog/the-critical-role-of-ssl-inspection-to-avoid-secure-malware-delivery, Apr. 2020.
〔48〕 Paloalto Networks, Unit 42 Cloud Threat Report, Volume 6, Apr. 2022.
〔49〕 MITRE, "Andariel", https://attack.mitre.org/groups/G0138/, Dec. 2023.
〔50〕 Verizon, "Data Breach Investigations Report", Jun. 2022.
〔51〕 AhnLab Security Emergency Response Center (ASEC), "Threat Trend Report on TeamTNT Group", AhnLab, Jul. 2021.

〈저자소개〉

김 해 나 (Hae-na Kim) 학생회원
2021 8월: 서울여자대학교 정보보호학과 학사
2021 8월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 보안공학, 위협모델링, 위험관리

김 예 준 (Ye-jun Kim) 학생회원
2019년 2월: 순천향대학교 정보보호학과 학사
2019년 3월~현재: 고려대학교 정보보호대학원 석박사통합과정
〈관심분야〉 보안공학, 위협모델링, 취약점 분석, 역공학

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년 한국인터넷진흥원(KISA) 팀장
2004년~2011년 성균관대학교 정보통신공학부 부교수
2011년~현재 고려대학교 정보보호대학원 정교수
2004년~현재 한국정보보호학회 이사
2014년~2015년 육군사관학교 초빙교수
2016년~2018년 개인정보분쟁조정위원회 위원
2017년~현재 고려대학교 국방RMF연구센터(AR²C) 센터장
2018년~현재 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2018년~2020년 대통령직속 4차산업혁명위원회 위원
2023년~현재 대통령직속 국방혁신위원회 위원
2023년~현재 고려대학교 디지털정보처 처장
2023년~현재 (사)한국국방혁신기술보안협회 협회장
〈관심분야〉 보안공학, 위협모델링, 보안성 평가/인증, DevSecOps, 암호학, 블록체인