블록체인과 제로 트러스트 기반 클라우드 보안 기법

나인혜[1], 강혁[2], 이근호[3*]
[1]백석대학교 컴퓨터공학부 학생
[2]고려대학교 영상정보처리협동과정
[3]백석대학교 컴퓨터공학부 교수

Cloud Security Scheme Based on Blockchain and Zero Trust

In-Hye Na[1], Hyeok Kang[2], Keun-Ho Lee[3*]
[1]Student, Division of Computer Engineering, Baek-Seok University
[2]Program in Visual Information Processing, Korea University
[3]Professor, Division of Computer Engineering, Baek-Seok University

요 약 최근 클라우드 컴퓨팅의 수요가 증가하고 자택근무 및 외부 업무로 인한 원격접속의 증가했다. 또한 외부 공격자의 접근뿐만이 아니라 내부 직원의 업무 접속과 같은 내부에서의 접근을 경계해야 할 필요성이 증가함과 동시에 다양한 공격 기법들이 고도화되는 현 상황에서 그에 맞는 새로운 보안 패러다임이 요구된다. 이로 인해 모든 것을 의심하고 신뢰하지 않는다는 핵심 원칙을 가진 제로 트러스트(Zero-Trust)를 적용한 네트워크 보안 모델이 보안업계에서 주목받기 시작했다. 제로 트러스트 보안은 모든 네트워크를 감시하고 접근을 허용 받기 위해선 먼저 인증을 받아야 하며 접근 요청자에 대한 최소한의 접근 권한을 부여함으로써 보안성을 높인다. 본 논문에서는 제로 트러스트와 제로 트러스트 아키텍처에 대해 설명하고, 제로 트러스트와 블록체인을 이용하여 기존 보안 시스템의 한계점을 극복하고 다양한 기업에서 활용할 수 있고 접근제어 강화를 위한 새로운 클라우드 보안 체계를 제안하고자 한다.

주제어 : 제로 트러스트, 클라우드, 블록체인, 정보보안, 기업보안

Abstract Recently, demand for cloud computing has increased and remote access due to home work and external work has increased. In addition, a new security paradigm is required in the current situation where the need to be vigilant against not only external attacker access but also internal access such as internal employee access to work increases and various attack techniques are sophisticated. As a result, the network security model applying Zero-Trust, which has the core principle of doubting everything and not trusting it, began to attract attention in the security industry. Zero Trust Security monitors all networks, requires authentication in order to be granted access, and increases security by granting minimum access rights to access requesters. In this paper, we explain zero trust and zero trust architecture, and propose a new cloud security system for strengthening access control that overcomes the limitations of existing security systems using zero trust and blockchain and can be used by various companies.

Key Words : Zero-Trust, Cloud, Blockchain, Information Security, Corporate Security

*본 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2020R1I1A3069008)
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2023년 01월 30일 수정일 2023년 2월 23일 심사완료일 2023년 2월 27일

1. 서론

최근 클라우드 컴퓨팅의 수요 증가와 함께 업무 형태의 다양화에 따라 각 산업 군에는 클라우드 보안의 중요성이 더욱 대두되고 있다. 하지만 외부 공격자뿐만 아니라 내부에서의 접근도 경계해야 할 필요성이 높아지면서[1], 기존의 보안 모델인 경계 기반의 접근 방식의 한계가 드러나고 있다. 이에 대한 대안으로 아무것도 신뢰하지 않는다는 가정하에 최소한의 권한으로 이루어지는 제로 트러스트(Zero-Trust) 보안이 주목받고 있으며, 이를 적용한 네트워크 보안 모델이 새로운 보안 패러다임으로 부상하고 있다[2]. 제로 트러스트 보안은 인증을 거쳐 최소한의 액세스만 허용하는 등 접근 제어를 강화하여 보안성을 높이는 것이 핵심 원칙이다[3].

본 논문에서는 제로 트러스트와 제로 트러스트 아키텍처에 대해 설명하고, 블록체인 기술과 제로 트러스트 보안 모델을 결합하여 새로운 클라우드 보안 체계를 제안하고자 한다.

2. 관련 연구

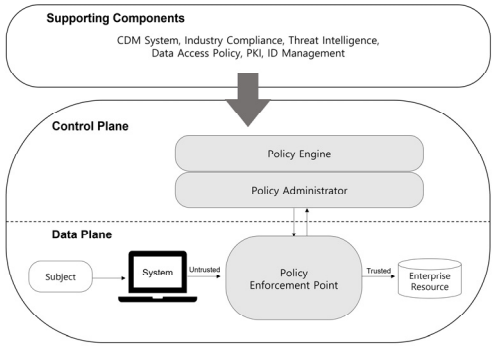
2.1 제로 트러스트 보안

제로 트러스트(Zero-Trust)는 모든 네트워크에 대한 접근 요청자에게 최소한의 접근 권한을 부여하여 보안성을 향상시킨다는 핵심 원칙을 가진 보안 모델이다[4]. 이 모델은 네트워크 안에 있는 모든 디바이스와 애플리케이션들을 신뢰하지 않는다는 전제로 시작되어 작동한다. 따라서 모든 디바이스와 애플리케이션은 접근 권한을 얻기 위해 인증을 받아야 하며, 인증이 이루어졌더라도 접근 권한은 최소화되어야 한다[5].

이러한 제로 트러스트 보안 모델은 클라우드 서비스에서 더욱 중요한 역할을 한다. 클라우드 서비스는 다양한 사용자와 디바이스가 자주 접근하는 복잡한 네트워크 환경에서 작동하므로[6], 기존의 보안 모델에서는 사용자나 디바이스를 신뢰하고 있어 보안에 취약할 수 있는 반면, 제로 트러스트 보안 모델은 사용자와 디바이스를 절대 신뢰하지 않으므로 보안 위협에 대해 더욱 적극적으로 대응할 수 있다.

Fig. 1과 같이 제로 트러스트 아키텍처는 크게 컨트롤 플레인과 데이터 플레인으로 나뉜다[7].

컨트롤 플레인(Control plane)은 네트워크 보안을 관리하고 제어하는 역할을 한다. 제로 트러스트 아키텍처



[Fig. 1] Zero-Trust Architecture

에서는 인증, 권한 부여, 인가 등의 제어를 컨트롤 플레인에서 처리한다. 이를 위해 보안 관리자는 인증 서버, 정책 서버, 권한 부여 서버 등과 같은 서버와 관리 도구를 구성한다. 이러한 컨트롤 플레인 구성을 통해 사용자와 장치의 신원을 인증하고, 접근 권한을 부여하고, 정책을 적용하여 네트워크 보안을 강화한다[8].

데이터 플레인(Data plane)은 컨트롤 플레인이 정의한 보안 규칙에 따라 실제 트래픽을 처리하는 역할을 한다. 제로 트러스트 아키텍처에서는 데이터 플레인에서 트래픽의 흐름과 데이터 플로우를 제어한다. 이를 위해 데이터 플로우의 기본 단위인 패킷(Packet)에 대한 보안 정책을 정의하고[9], 이를 기반으로 네트워크 장비들에 대한 Access Control List(ACL) 등의 제어 규칙을 적용한다. 데이터 플레인은 이러한 보안 정책에 따라 데이터를 처리하여, 안전한 데이터 통신을 보장한다.

Policy Engine은 제로 트러스트 모델에서 보안 정책을 작성, 구성 및 관리하는 역할을 한다. 이러한 Policy에서는 액세스 권한 및 규칙, IP 주소 및 기타 규칙을 정의하며 데이터 흐름을 관리한다. Policy Administrator는 정책 엔진에서 사용되는 정책 구성을 관리하고 업데이트하는 역할을 한다. 이러한 요소는 일반적으로 관리자에게 인터페이스를 제공하여 정책 설정을 쉽게 할 수 있도록 한다. 마지막으로 Policy Enforcement Point (PEP)는 인증 및 권한 부여 프로세스를 통해 액세스를 요청하는 클라이언트와 실제로 데이터를 보호하고 있는 데이터 플레인 간의 중개자 역할을 한다. 이러한 요소는 일반적으로 네트워크 장비나 애플리케이션과 같은 다양한 보안 시스템을 의미한다. subject는 자원을 이용하려는 주체이며, subject는 Policy Decision Point에서 인증을 받고, identity와 context에 따라 해당 subject에 최소한의 권한만 부여받는다. subject는 앞서 부여받은

권한에 따라 Policy enforcement point에 의해 기업 자원에 접속하게 되는 것이다[10].

이러한 구성 요소를 통해 사용자가 클라우드 서비스를 이용할 때마다 보안성을 검증하여 안전한 클라우드 환경을 제공합니다. 이 모델은 모든 사용자와 기기를 신뢰하지 않는 것이 기본 전제로, 모든 요청에 대해 세밀한 검증과 인증을 수행하여 보안성을 강화한다.

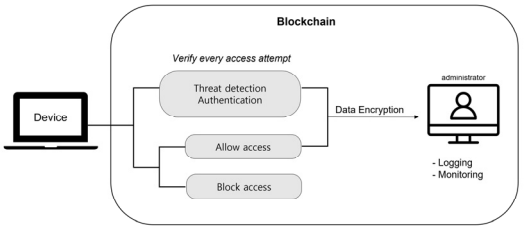
2.2 기존 클라우드 시스템의 한계점

경계 기반(perimeter-based)의 접근 방식은 내부 네트워크와 외부 네트워크 사이에 경계를 만들어, 외부에서 내부로의 접근을 통제하는 방식이다. 이 방식은 내부 네트워크를 보호하기 위해 방화벽, 침입 탐지 시스템, 가상 사설망(VPN) 등을 사용한다[11].

그러나 클라우드 서비스에서는 이러한 경계 기반의 보안 방식이 제한적인 역할을 하기 때문에 한계점이 있다. 클라우드 서비스는 다양한 디바이스와 네트워크에서 접근 가능하기 때문에, 네트워크 경계를 만들어 놓는 것만으로는 보안을 충분히 보장할 수 없다. 또한, 내부 네트워크와 외부 네트워크 사이의 경계가 모호해지기 때문에[12], 이를 효과적으로 관리하기 어렵다.

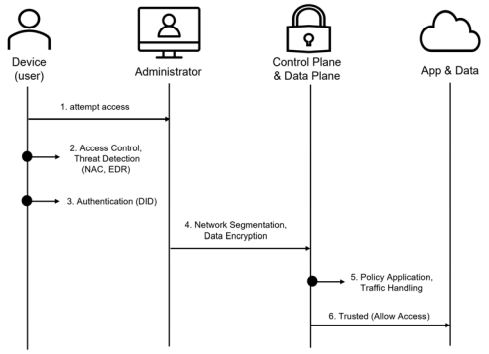
3. 시스템 설계

제로 트러스트 보안 모델을 적용한 클라우드 서비스의 핵심은 비인가 사용자의 접근 차단이 아니라 접근하려는 주체에 대한 엄격한 검증과 최소한의 접근만을 허용하여 해당 주체만을 집중적으로 감시하는 것이다. 접근 허가된 사용자에게도 지속적인 네트워크 모니터링으로 제로 트러스트 모델 기반의 클라우드 서비스를 실현해야 한다. 다음 Fig. 2와 같이 블록체인 기반의 제로 트러스트를 통한 클라우드 서비스의 구성도를 제시한다.



[Fig. 2] Service Diagram

본 논문에서 제안하는 서비스는 제로 트러스트 보안 모델을 적용함으로써, 최소한의 접근 권한을 부여받도록 설계되어 있기 때문에 데이터 보안성과 안전성을 보장한다. 또한 민감한 정보에 대해서는 데이터 송수신 가능한 경로를 정하여 안전하게 전송할 수 있으며 업무의 효율성을 위해 자동화된 접근 정책의 토대를 마련하게 된다. 또한 지속적인 네트워크 모니터링으로 제로 트러스트 모델 기반의 클라우드 서비스를 실현한다. 다음 Fig. 3와 같이 블록체인 기반의 제로 트러스트를 통한 클라우드 서비스의 프로세스를 제시한다.



[Fig. 3] System Process

자세한 프로세스는 다음 순서를 따른다.

① 위협 탐지 및 접근 제어

NAC(Network Access Control)는 네트워크에 접근하는 모든 디바이스들이 먼저 인증된 후에 허가된 장치만 네트워크에 접근할 수 있도록 제어하는 기술이다. 이를 위해서는 네트워크 상의 각각의 디바이스에 NAC Agent를 설치하여 인증 프로세스를 수행해야 한다. 정의된 NAC 보안 정책에 맞게 Endpoint가 준비되었을 때 내부망과 인터넷에 접근이 가능하다[13]. 이를 통해 네트워크에 접속하는 장치의 신원을 확인하고, 네트워크에 연결된 디바이스의 보안상태를 검사하여 취약점이 발견될 경우 차단하거나 이를 보안 업데이트로 해결할 수 있도록 한다.

EDR(Endpoint Detection and Response)은 단말기에서 발생하는 모든 이벤트를 실시간으로 모니터링하고 분석하는 기술이다[14]. 이를 통해 시스템 내부의 위협을 신속하게 탐지하고 대응할 수 있다. EDR은 악성코드 탐지, C&C와의 통신 탐지, 비정상적인 프로세스 동

작 탐지 등의 기능을 수행한다. EDR 시스템은 기본적으로 Endpoint Agent를 설치하여 단말기에서 발생하는 모든 이벤트를 수집하고 분석한다.

이와 같이 NAC와 EDR을 활용하여 접근자의 단말기에 대한 감시 및 감독을 통해 비인가된 사용자나 장치의 접근을 차단할 수 있다. 이는 네트워크 보안을 강화하고, 민감한 데이터에 대한 보호 수준을 높이는 데에 도움이 된다. 또한 네트워크 내부에서 발생할 수 있는 보안 위협을 탐지하고 대응할 수 있으며 악성코드, 스파이웨어 등의 위협을 탐지하고 사전 차단함으로써 클라우드 서비스의 안정성을 높이는 데에 도움이 된다.

② DID를 통한 신원인증

DID(Decentralized Identity)는 블록체인을 기반으로 사용자 신원을 인증하는 기술이다. DID는 블록체인 기술을 기반으로 생성된 고유한 식별자로, 이 고유한 ID는 블록체인과 같은 분산 원장 기술에서 생성되며, 일반적으로 암호화폐의 지갑 주소와 비슷한 형식을 갖는다. DID를 사용하면 보를 분산해서 신원을 위한 최소한의 정보만을 선택해 증명할 수 있어 인증 과정에서 안전하게 자신의 신원 정보를 직접 관리할 수 있으며, 중개자 없이 주체적으로 다른 사람과 안전하게 공유할 수 있다.

먼저, 사용자는 클라우드 서비스를 이용하기 위해 DID(Distributed Identifier)를 이용하여 신원 인증을 진행한다. 사용자가 클라우드 서비스에 접속할 때 블록체인 네트워크에 등록된 사용자 정보를 검증한다. 사용자 인증 정보를 블록체인에 저장하고, 사용자가 인증을 요청하면 블록체인에서 해당 정보를 검색하여 인증을 수행한다. 블록체인 기반 신원 인증은 탈 중앙화된 구조와 블록체인의 보안성, 불변성, 안전성을 이용하여 안전한 인증 시스템을 구축한다.

③ Network Micro-Segmentation

인증이 완료되면, 사용자가 원하는 클라우드 서비스를 선택한다. 선택된 서비스 인스턴스는 제로 트러스트 보안 모델에 따라 마이크로 서비스로 분할된다. 이때, 선택된 서비스 인스턴스는 필요에 따라 여러 개의 마이크로 서비스로 분할될 수 있다. 각 마이크로 서비스는 단일 기능을 수행하며, 서로 독립적으로 실행된다.

클라우드 서비스는 사용자의 인증을 기반으로 적절한 접근 권한을 부여한다. 이때, 제로 트러스트 보안 모델에 따라 권한이 부여된다. 제로 트러스트 보안 모델은 가장 작은 권한을 가진 서비스가 필요한 권한만을 가지고 접근할 수 있도록 설계되어 있다. 따라서, 세그먼트 단위로 세분화하여 대상을 통제하기에 사용자가 필요로 하는 마이크로 서비스만 사용 가능하다.

Network Micro-Segmentation은 제로 트러스트 모델의 핵심 보안 메커니즘 중 하나이다[15].

이는 네트워크 환경을 여러 개의 작은 영역으로 분할하고, 각각의 영역에 대해 허용된 액세스만 허용하는 것을 의미한다. 이를 통해 어떤 영역이든 다른 영역에 대한 접근을 엄격하게 제어하고, 비인가된 사용자의 침입을 제어하여 전체 시스템의 보안을 강화할 수 있다. Micro-Segmentation은 기본적으로 네트워크를 가상화하여 작동한다. 가상 네트워크는 물리적인 네트워크와 분리되어 있으며, 가상화된 네트워크 단위 안에서만 트래픽이 발생한다. 이를 통해 가상 네트워크 내에서 트래픽을 추적하고, 필요한 경우에만 노출시켜 세밀한 제어를 가능하게 한다. 가상 네트워크 내의 각각의 세그먼트는 자체적인 보안 규칙을 갖고 있으며, 이를 통해 세그먼트 간의 트래픽을 허용하거나 차단할 수 있다. 예를 들어, 데이터베이스 서버가 있는 세그먼트에 대한 액세스를 허용하기 위해서는 해당 세그먼트로부터의 트래픽에 대해 명시적으로 허용 규칙을 작성해야 한다. 이를 통해 제로 트러스트 보안 모델에서는 필요한 액세스만을 허용하고, 이외의 접근은 차단함으로써 보안을 강화할 수 있다.

④ 데이터 암호화 및 보안

클라우드 서비스의 모든 데이터는 블록체인 기술을 사용하여 분산 원장에 기록된다. 블록체인 기술은 중앙 집중형 시스템과는 달리 분산 원장 구조를 사용하여 데이터 무결성을 보장한다. 이를 통해 데이터가 위변조되거나 삭제될 수 없다.

사용자는 클라우드 서비스를 사용하여 데이터를 생성, 수정 또는 삭제할 수 있다. 이러한 작업은 블록체인 기술을 사용하여 데이터 무결성이 보장되며, 제로 트러스트 모델을 사용하여 사용자가 액세스할 수 있는 데이터의 범위를 제한할 수 있다.

데이터가 클라우드 서비스에서 제거되면 블록체인에도 이를 반영하도록 해야 한다. 이를 위해 블록체인에 데이터를 추가하는 것 외에도, 제로 트러스트 모델을 사용하여 사용자에게 삭제 권한을 부여하여 데이터가 클라우드 서비스에서 완전히 삭제될 수 있도록 해야 한다.

클라우드 서비스에 보관되는 모든 데이터는 블록체인에서 기록되며, 블록체인에서 이러한 트랜잭션은 블록체인의 모든 노드에 동기화된다. 이를 통해 데이터 무결성

이 보장되며, 중앙 집중형 시스템과 달리 데이터 위변조 또는 삭제를 방지할 수 있다.

마지막으로, 분할된 마이크로 서비스에서 생성되는 데이터는 제로 트러스트 보안 모델에 따라 암호화되어 저장된다. 암호화된 데이터는 클라우드 서비스 내부에서만 처리되며, 외부로 노출되지 않는다. 이러한 데이터 암호화는 클라우드 서비스 제공 업체와 사용자 간에 데이터 무단 액세스를 방지하는 데 큰 역할을 한다.

마이크로 서비스 간 통신은 제로 트러스트 보안 모델에 따라 강력한 보안 절차를 거쳐 이루어진다. 각 마이크로 서비스는 클라우드 서비스 내부의 다른 마이크로 서비스와 통신할 때, 제로 트러스트 보안 모델에 따라 보안 절차를 거쳐 통신한다. 이를 통해 외부에서의 공격으로부터 보호할 수 있다.

제로 트러스트 보안 모델은 모든 클라우드 서비스의 활동을 감시하고, 보안 위반 사항이 발생하면 즉시 대응한다. 클라우드 서비스는 로깅, 감사 및 분석을 수행하여 모든 활동을 추적하고, 보안 위반 사항을 탐지한다. 이를 통해 보안 위반 사항이 발생할 경우 신속한 대응이 가능하다.

제로 트러스트 보안 모델은 클라우드 서비스의 보안을 유지하기 위해 주기적인 업데이트 및 유지 보수를 수행한다. 클라우드 서비스는 보안 업데이트 및 유지 보수를 자동으로 수행하며, 이를 통해 보안 위협으로부터 안전하게 보호된다.

〈Table 1〉 Performance comparison with existing system

	Existing Cloud Service	Cloud Service with Zero Trust
Confidentiality	X	O
Throughput	Low	High
Expense	Low	High
Resource Usage	High	Low
Response Time	Long	Short

〈Table 1〉은 기존 클라우드 시스템과 본 논문에서 제안하는 시스템을 비교한 표이다. 비교 항목은 Confidentiality(기밀성), Throughput(처리량), Expense(비용), Resource Usage(자원 사용량), Response Time(응답 시간)으로 나뉜다. Confidentiality는 데이터나 자원의 비밀 유지 및 불법적인 접근 방지 여부를 의미하고 Throughput은 단위 시간당 처리 가능한 데이터양을 의미하며, Expense는 시스템 구축, 운영, 유지 보수 등에 소요되는 비용을 의미한다. Resource Usage는 시스템 구성에 필요한 하드웨어, 네트워크, 소프트웨어 등의 자원 사용량을 의미하며, Response Time은 요청한 작업에 대한 응답시간을 의미한다. 〈Table 1〉과같이 본 논문에서 제안하는 서비스는 기존의 경계 기반 접근 방식의 클라우드 서비스와 비교했을 때, 분산 네트워크와 암호화 기술을 이용하여 데이터의 위변조, 도난, 손상, 위험 등에 대한 보안 수준이 높아지고, 접근 권한이 엄격하게 제어되기 때문에 불법적인 접근을 차단할 수 있다. 이를 통해 데이터 무결성과 기밀성이 보장되며, 클라우드 서비스의 신뢰성이 향상된다. 또한 블록체인 기술을 활용한 분산 데이터 처리로 인한 처리 속도가 향상될 것으로 보이며, 분산 네트워크를 이용하기에 자원 공유 및 최적화가 가능하고, 응답 속도가 빠른 환경 구축이 가능하다. 하지만 제안하는 서비스는 보안성을 높이기 위해 추가적인 인프라 및 기술이 필요하므로 초기 구축 비용이 더 많이 들 수 있다. 그러나 보안 위협으로 인한 손실 방지 효과를 고려할 때 장기적으로는 효율적인 선택일 것으로 기대된다.

4. 결론

본 논문에서는 제로 트러스트 아키텍처에 대해 설명하고 블록체인 기술과 제로 트러스트 보안 모델을 결합한 새로운 클라우드 보안 체계를 제안하였다. 제로 트러스트 보안 모델과 블록체인 기술을 결합한 클라우드 보안 체계는 클라우드 보안의 새로운 패러다임을 제시하며, 기존의 클라우드 보안 모델에서 발생하던 문제점들을 해결할 수 있는 대안으로 주목받을 것으로 예상된다. 또한 제로 트러스트는 모든 접근을 의심하고 엄격한 보안을 요구하는 핵심 원칙을 가지고 있기 때문에 원격 접속 보안을 위한 대안으로 강력하게 대두되고 있으며 이러한 이점으로 인해 제로 트러스트 보안은 다양한 기업들의 보안 문제에 대한 해결책으로 제안되고 있다. 그러나 제로 트러스트 보안 모델이 현재 IT 보안에 대한 중요한 패러다임 변화를 가져오고 있지만, 이를 적용하기 위해서는 기업 내에서 제로 트러스트 보안 모델을 적용한 기업의 보안 시스템 구축 가능성과 사례 및 한계에 대한 연구를 진행해야 하며, 제로 트러스트 보안 모델과 블록체인 기술의 시너지 효과와 경제적 효과를 분석해야 한다. 또한 보안 시스템을 구축할 인적 자원의 확보와 기업 환경에 대한 추가적인 연구가 필요하다. 본 논문은 제로 트러스트 보안과 블록체인 기술이 클라우드 보안 분야에서 유용하게 활용될 수 있음을 보여주며, 앞으로 더욱 발전된 클라우드 보안 체계의 구축에 기여할

것으로 기대된다. 따라서 기업들은 제로 트러스트에 대한 꾸준한 논의와 분석을 통해 안전한 클라우드 보안 체계를 구축해야 할 것이다.

REFERENCES

[1] J. H. Lee and H. Y. Kwon, "A Study on Human Vulnerability Factors of Companies : Through Spam Mail Simulation Training Experiments" The Journal of Korea Institute Of Information Security And Cryptology, vol. 29, no. 4, pp. 847-857, Aug. 2019.

[2] S. Bal, C. Cun, and P. Cer, "Five Steps To A Zero Trust Network : Zero Trust Is The Blueprint For Your Security Architecture" Forrester Research Report, Oct. 2018.

[3] Y. J. Jeon, "Security and Trust on Non-Contact Financial Transaction", Digital Convergence Journal, Vol.19, No.7, pp.147-154, 2021.07.

[4] Cisco, "Cisco Duo Security Zero Trust Solution for User and Device Security", CISCO systems Korea Ltd, Seoul, 2020

[5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, 2020.

[6] S. Y. Kim, K. H. Jeong, Y. N. Hwang, and D. H. Nyang, "Abnormal Behavior Detection for Zero Trust Security Model Using Deep Learning" Korea Information Processing Society Collection of academic papers, Vol.28, No.1, pp.132-135, 2021.

[7] J. Y Chun, Zero trust basis of network security strategy, IDG Summary AKAMAI MEGAZONE, 2021.

[8] A. Kerman, O. Borchert, S. Rose, and A. Tan, Implementing a zero trust architecture, The MITRE Corporation, Tech. Rep, 2020.

[9] M. J. Hwang, Microsoft Zero Trust Network Strategy and Implementation Plan, Microsoft Cyber Security Solutions Group, 2020.

[10] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access Control Policy Enforcement for Zero-Trust-Networking" 2018 29th Irish Signals and Systems Conference (ISSC), pp.1-6, 2018.

[11] R. Riccardo and M. Repetto, "Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model" Future Generation Computer Systems, Vol.85, pp.235-249, 2018.

[12] H. B. Chang, "A Study on The Countermeasure by The Types through Case Analysis of Industrial Secret Leakage Accident" Convergence security journal, Vol.15 No.7, pp.39-45, 2015

[13] G. Anil, "A Zero-Trust Security Framework for Granular Insight on Blind Spot and Comprehensive Device Protection in the Enterprise of Internet of Things (E-IOT)" BMS Institute of Technology, 2021.

[14] K. D. Uttecht, "Zero Trust (ZT) Concepts for Federal Government Architectures" Massachusetts inst of tech lexington United States, 2020.

[15] Chou, T. S. "Security threats on cloud computing vulnerabilities" International Journal of Computer Science & Information Technology, pp. 79-88, 2013.

나 인 혜(In-Hye Na) [준회원]

■ 2020년 3월 ~ 현재 : 백석대학교 정보보호학과 재학

〈관심분야〉
정보보안, 네트워크보안, 블록체인, 개인정보보호

강 혁(Hyeok Kang) [종신회원]

■ 2013년 3월 : 위싱턴대학교 컴퓨터학과(박사수료)
■ 2020년 9월 ~ 현재 : 고려대학교 박사과정
■ 2015년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
양자암호, 융합 보안, 생체 인증, 블록체인

이 근 호(Keun-Ho Lee) [종신회원]

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

〈관심분야〉
이동통신 보안, 융합보안, 개인정보보호, 블록체인