creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

이 일 구 교수 지도
석사학위 청구논문

저지연 고신뢰 네트워크 서비스를 위한 동적 제로 트러스트 클라우드 구조 및 접근 제어 메커니즘

2024

성신여자대학교 대학원
미래융합기술공학과
김 소 희

저지연 고신뢰 네트워크 서비스를 위한 동적 제로 트러스트 클라우드 구조 및 접근 제어 메커니즘

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2023년 11월

성신여자대학교 대학원

미래융합기술공학과

김 소 희

인 준 서

김소희의 석사학위 논문으로 인준함

2023년 11월

심사위원장 임 연 섭 (인)

심 사 위 원 이 주 희 (인)

심 사 위 원 이 일 구 (인)

성신여자대학교 대학원

논 문 개 요

클라우드 컴퓨팅 장치들이 초고속 네트워크에 연결되고 네트워크 경계가 사라지게 되면서, 디지털 자산을 안전하게 보호하기 위해 종래의 경계 기반 접근 제어 방식의 한계를 극복할 수 있는 제로 트러스트 기반의 접근 제어 방식이 클라우드 보안의 새로운 패러다임으로 떠올랐다. 제로 트러스트는 아무도 신뢰하지 않고, 클라우드 자원에 접근할 때마다 사용자에 대한 엄격한 신뢰도 평가 절차를 수행함으로써 높은 수준의 보안을 제공하지만, 지속적인 평가와 모니터링 절차 때문에 서비스 처리 지연 시간을 증가시키는 트레이드오프 문제가 있다. 그러나 초저지연 네트워크 환경에서 지연에 민감한 서비스를 원활하게 지원하기 위해서는 보안과 성능의 트레이드오프 관계를 최적화해야 한다. 본 논문에서는 보안과 성능을 동시에 보장하기 위해 프라이버시 민감도와 지연 민감도에 따라 사용자 신뢰도 평가 절차가 다른 세 가지 클라우드 접근 제어 정책을 동적으로 적용하는 DZTA(Dynamic Zero Trust Architecture)를 제안한다. 종래 기술과 DZTA의 종단 간 지연 시간 및 공격 파급력을 비교 평가하기 위해 클라우드 접근 제어 정책의 효과를 수학적으로 모델링했고, 수치 분석 결과를 기반으로 성능을 분석했다. 그 결과 DZTA는 종래 ZTA(Zero Trust Architecture) 대비 지연 시간이 평균 85% 감소했고, 공격 파급력은 경계 기반 접근 제어 방식 대비 평균 8200% 감소했다.

목 차

표 차 례

그림 차례

Ⅰ. 서 론

클라우드 컴퓨팅은 디지털 혁신의 핵심 인프라로써 산업 및 디지털 기술과 융합하며 고부가가치를 창출하고 있다[1-3]. 많은 기업이 비즈니스 경쟁력을 확보하기 위해 클라우드 도입을 추진하고 있으며[4], 국가적 차원에서도 혁신적인 서비스 제공을 위해 클라우드 전략을 채택하고 있다[5-7]. Statista에 따르면, 2023년부터 2028년까지 퍼블릭 클라우드 산업의 글로벌 매출은 약 4,700억 달러 규모로 성장할 것으로 전망된다[8]. 이처럼 클라우드 기술이 범지구적으로 보편화되면서 클라우드 보안 문제가 주요 과제로 떠올랐다[9-11]. 가상화, 멀티 테넌시, 분산 저장 등 온프레미스 환경과 다른 클라우드 환경의 새로운 특성은 보안 취약점을 초래했다[12]. 데이터 및 서비스가 여러 위치에 분산 저장되고 다수의 테넌트가 동일한 서버를 공유하면서 접근 제어가 복잡해졌고, 클라우드 서비스 제공자(CSP) 및 공유 테넌트와 같은 내부자에 의한 공격도 가능해졌다[13-15]. 또한, 클라우드를 기반으로 수많은 모바일 장치가 연결되면서 측면 이동을 통한 공격 확산의 파급력이 기하급수적으로 커졌다[16]. 네트워크 환경이 변화함에 따라 전통적인 경계 기반 접근 제어 방식은 한계에 직면했고, 자원 단위로 접근을 제어하는 제로 트러스트 개념이 보안의 새로운 패러다임으로 떠올랐다[17].

제로 트러스트는 "절대 신뢰하지 말고, 항상 검증하라"를 대원칙으로 하는 새로운 보안 개념이다[18]. 제로 트러스트는 네트워크의 위치와 관계없이 모든 사용자를 신뢰하지 않으며, 데이터 및 서비스에 접근할 때마다 사용자를 평가하고 접근을 제어한다[19, 20]. 개별 자원 단위로 접근을 제어하기 때문에 측면 이동을 통한 공격의 확산을 방지할 수 있으며[21], 모든 사용자를 신뢰하지 않고 항상 검증하므로 대규모 클라우드 환경에 연결된

수많은 사용자에 대한 효과적인 접근 제어가 가능하다[22]. 이처럼 제로 트러스트가 클라우드 환경의 보안 문제를 해결할 수 있는 기술로 주목받으면서[23], 이를 국가 사이버 보안 전략으로 채택하는 국가가 증가하였다. 미국을 중심으로 유럽, 영국, 한국, 일본 등 다양한 국가가 국가적 차원의 제로 트러스트 개발 및 도입을 적극적으로 추진하고 있으며, 대규모의 국가 예산을 투입하고 있다. 하지만, 이러한 노력에도 불구하고 글로벌 제로 트러스트 도입률은 여전히 낮은 수준에 머물러 있다[24]. 전문가들은 제로 트러스트의 지속적이고 복잡한 사용자 신뢰도 평가 절차가 유발하는 서비스 지연 시간이 산업 현장에 클라우드를 도입하고 활용하기 어렵게 한다고 지적한다[25, 26]. 초고속 초저지연 네트워크 환경에서 지연 시간 문제는 매우 중요하며, 의료 시스템, 스마트 팩토리, 자율주행자동차 등에서는 생명과 직결된 문제를 초래할 수 있다[27]. 따라서, 미션 크리티컬 애플리케이션을 지원하기 위해서는 초저지연을 보장하는 것이 매우 중요하다[28].

본 연구에서는 제로 트러스트 환경에서 보안과 성능의 트레이드오프를 최적화하는 문제에 초점을 맞춘다. 일반적으로 보안과 성능은 하나가 강화되면 다른 하나가 약화되는 상충 관계에 놓여있다고 알려져 있다[27]. 제로 트러스트 역시 지속적인 사용자 신뢰도 평가 절차로 보안을 강화하는 동시에 지연 시간을 증가시켰다. 그러나 지연에 민감한 서비스를 지원하기 위해서는 제로 트러스트의 사용자 신뢰도 평가 절차 지연 문제를 해결해야 한다[29]. 이러한 배경에서 본 연구는 보안과 성능을 최적화하는 동적 제로 트러스트 아키텍처와 접근 제어 메커니즘을 제안한다.

본 논문의 나머지는 다음과 같이 구성된다. 2장에서는 제로 트러스트의 개념과 구조 및 동작 원리를 설명하고, 3장에서는 주요국의 클라우드 접근 제어 정책과 제로 트러스트 운영 실태 및 한계점을 분석한다. 4장에서는 초저지연 네트워크 서비스 요구사항에 대하여 분석하고, 5장에서는 선행

연구를 분석한다. 6장에서는 제안하는 동적 제로 트러스트의 개념, 구조 및 동작 원리를 설명하고, 7장에서는 수학적 모델링을 바탕으로 성능 평가를 수행한다. 8장에서는 동적 제로 트러스트 아키텍처의 기대효과를 제시하고, 마지막 9장에서는 결론을 맺고, 향후 연구 계획을 제시한다.

Ⅱ. 클라우드 접근 제어 기술 분석

1. 제로 트러스트 개념

제로 트러스트라는 용어는 John Kindervag에 의해 처음 등장했다. Kindervag는 한 연설에서 암묵적 신뢰는 곧 취약성이며, 모든 사용자를 신뢰하지 말아야 한다고 주장했다. 그리고 2010년, Kindervag는 Forrester Research의 보고서를 통해 제로 트러스트 개념을 정의했다[30]. 이 보고서에서 네트워크 위치와 관계없이 모든 자원에 대해 접근을 제어하고, 최소한의 접근 권한만 부여하며 주기적으로 검증하면서, 지속적으로 트래픽을 검사하고 기록하는 것을 제로 트러스트의 기본 개념으로 제시했다[31]. 이후 제로 트러스트 개념은 지속적으로 발전하고 구체화되었다.

전통적인 산업이 디지털 환경으로 전환되면서 기업의 업무 환경은 다변화했으며, 클라우드 및 원격 근무가 보편화되면서 내부와 외부의 경계가 사라졌다. 경계 기반 접근 제어 방식은 더 이상 공격에 충분히 대응하지 못하고 있으며, 내부 확산 공격으로 인한 대규모 피해는 해마다 증가하고 있다[32]. 이러한 상황 속에서 제로 트러스트는 경계 기반 접근 제어 방식을 대체할 새로운 메커니즘으로 떠올랐다. 2020년 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 SP 800-207 보고서를 통해 제로 트러스트 아키텍처를 발표했으며, 이 문서를 통해 7가지 제로 트러스트의 기본 원리를 제시했다. 1) 모든 데이터, 장치, 서비스를 자원으로 간주하며, 2) 네트워크의 위치와 관계없이 모든 접근 요청을 신뢰하지 않는다. 3) 자원에 대한 접근은 세션 단위로 허가하며, 4) 접근 요청은 동적 정책에 따라 사용자의 행위, 환경, 정보 민감도를 고려하여 결

정한다. 5) 기업은 모든 자산을 신뢰하지 않으며, 디바이스 및 애플리케이션의 상태를 지속적으로 모니터링한다. 6) 모든 자원의 인증과 인가를 강력하게 수행하며, 7) 자산, 네트워크, 트래픽 정보를 최대한 많이 수집한다[33].

2. 제로 트러스트 구조와 동작 원리

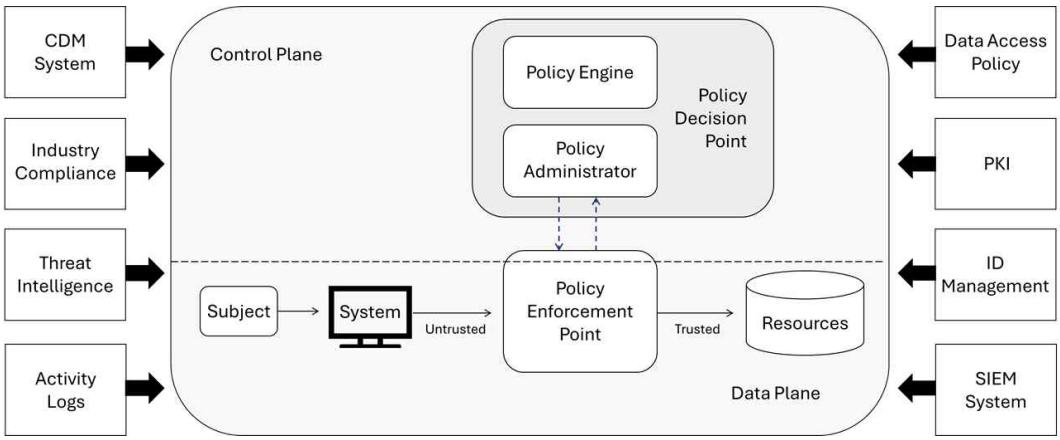

FIGURE 1. Zero trust architecture[33]

Fig. 1은 NIST SP 800-207 보고서에서 제시한 ZTA(Zero Trust Architecture)이다. ZTA는 정책을 결정하는 컨트롤 플레인과 정책을 집행하는 데이터 플레인으로 나누어진다. 접근 제어 정책을 결정하고 집행하는 핵심적인 기능을 하는 영역은 정책 결정 지점과 정책 집행 지점이며, 정책 결정 지점은 정책 엔진과 정책 관리자로 구성된 두 개의 논리적 컴포넌트를 포함하고 있다. 정책 엔진은 자원에 대한 접근 허용 또는 거부를 결정하며, 정책 관리자는 정책 엔진의 결정에 따라 인증과 인가 토큰을 발행하

고 이를 정책 집행 지점에 보낸다. 정책 집행 지점은 정책 관리자와 통신하며 정책을 업데이트하고, 사용자와 자원을 연결하거나 연결을 종료한다. 또한, 정책 엔진은 접근 요청을 처리할 때, 사용자의 신뢰도를 평가하기 위해 다양한 외부 데이터 소스를 활용하는데, 대표적으로 기업의 보안 상태를 수집 및 분석하는 SIEM과 새로운 공격 및 취약점 등에 관한 정보를 제공하는 위협 인텔리전스, 사용자를 식별하기 위한 ID 관리 시스템 등이 있다. 자원은 마이크로 세그멘테이션을 통해 각 세그먼트에 개별 자원 또는 소규모 자원 그룹을 배치하는 방식으로 관리할 수 있다[33].

Ⅲ. 클라우드 접근 제어 정책 분석

1. 주요국의 클라우드 접근 제어 정책 분석

제로 트러스트 접근 제어 정책을 가장 적극적으로 추진하고 있는 국가는 미국이다. 미국 바이든 행정부는 2021년 5월에 사이버 보안 능력 강화를 골자로 하는 행정명령(Executive Order 14028)인 「Improving the Nation's Cybersecurity」를 발표했다. 클라우드 및 온프레미스 환경에서 자산을 안전하게 보호하기 위해 정부 기관의 클라우드 시스템에 제로 트러스트 접근 제어 정책의 적용을 의무화했다[34]. 이를 위해 NIST, CISA(Cybersecurity & Infrastructure Security Agency), OMB(Office of Management and Budget) 등에 제로 트러스트 아키텍처에 관한 명확한 지침 마련을 지시했고, 이에 따라 CISA는 제로 트러스트 성숙도 모델을 개발하여 발표했다[35]. OMB는 「Moving the U.S. Government Toward Zero Trust Cybersecurity Principle」를 발표했고[36], NIST는 「Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators 」와 제로 트러스트 아키텍처 구현 보고서 시리즈를 발간했다[37-41]. 또한, 미국은 제로 트러스트 구현을 위한 대규모 투자도 감행하고 있다. 2024년도 미국 회계연도(FY) 예산을 살펴보면, IRM(Information Resource Management) 자금이 39.6만 달러 증액되었는데, 이 중 30만 달러가 사이버 보안 지원 및 제로 트러스트 아키텍처 개선에 편성되어 있다. 또한, CIF(Capital Investment Fund)의 IT(Information Security) 부문 요청액은 9,550만 달러 규모이며, 해당 부문은 제로 트러스트 이니셔티브로의 혁신을 핵심 목표로 하고 있다[42].

유럽 연합은 NIS2(Network and Information System 2) 지침을 통해 핵심 기관의 클라우드를 비롯한 디지털 인프라 보호를 위해 제로 트러스트 원칙을 채택하고, 신원 및 접근 관리를 철저히 해야 한다고 규정했다[43]. 또한, 연구 및 혁신 자금 지원 프로그램 Horizon Europe을 통해 연결된 의료 기기의 사이버 보안을 개선하기 위한 ENTRUST(ENsuring Secure and Safe CMD Design with Zero TRUST Principles) 프로젝트를 추진하고 있다. 이 프로젝트는 자원이 제한된 실시간 시스템에서도 제로 트러스트를 효과적으로 구현할 수 있는 메커니즘 개발을 목표로 하고 있다[44].

신 보안체계 도입은 한국 정부의 주요 국정 과제 중 하나인 디지털 플랫폼 정부의 핵심 추진 과제이다[45]. 정부의 시스템이 클라우드 기반의 개방·공유 환경으로 변화하면서 이에 적합한 새로운 보안 체계가 필요하게 된 것이다. 한국은 제로 트러스트 전략을 채택하고, 과학기술정보통신부(Ministry of Science and ICT, MSIT)와 국가정보원, 행정안전부의 주도로 제로 트러스트 도입을 추진하고 있다. MSIT는 2022년 10월 제로 트러스트 포럼을 발족하고 「제로 트러스트 가이드라인 1.0」을 발표하였으며[46], MSIT와 한국인터넷진흥원(Korea Internet & Security Agency, KISA)은 한국형 제로 트러스트(K-Zero Trust) 모델을 발굴하기 위해 제로 트러스트 보안 실증 지원사업을 수행하고 있다[47].

일본은 「디지털 사회 실현을 위한 중점 계획」을 통해 "Cloud by default"를 행정 서비스의 온라인 실현을 위한 기본 원칙으로 설정하였다[48]. 이로 인해 온-프레미스 환경과 다른 새로운 위협에 대응할 필요성이 증가하였고, 제로 트러스트를 사이버 보안 전략으로 채택하였다. 일본 디지털청은 「제로 트러스트 아키텍처 적용 정책」을 발표하며 제로 트러스트 아키텍처를 적용하기 위한 기본 방침 및 유의 사항을 제시하였다[49]. 그리고 문부과학성(Ministry of Education, Culture, Sports, Science and

Technology, MEXT)은 「디지털 사회 실현을 위한 중점 계획에 근거한 문부과학성의 중장기 계획」을 발표하며 문부과학성의 행정 시스템은 제로 트러스트 아키텍처를 염두에 둔 형태로 구성되어 있으며, 고위험 시스템을 시작으로 제로 트러스트 기반 인증 체계를 도입 및 확대해 나갈 계획이라고 밝혔다[50].

싱가포르는 정부의 디지털 혁신 및 클라우드 우선 전략 채택으로 사이버 위협이 증가하면서, 이에 대응하기 위한 목적으로 「The Singapore Cybersecurity Strategy 2021」를 통해 CII(Critical Information Infrastructure)에 제로 트러스트 원칙을 채택할 것을 권장하였다. 또한, 정부의 사이버 보안 아키텍처 현대화를 위해 제로 트러스트 원칙을 싱가포르 정부의 실정에 맞게 변형한 GTbA(Government Trust-based Architecture)를 구현하였다[51]. 그리고 「Cybersecurity Code of Practice for Critical Information Infrastructure」에 CIIO(CII Owner)로 하여금 제로 트러스트 원칙을 채택할 것을 강하게 권고하는 항목을 추가하였다[52].

2. 주요국의 제로 트러스트 클라우드 운영 실태 분석

주요국들이 제로 트러스트 도입을 적극적으로 추진하고 있는 가운데, 글로벌 제로 트러스트 도입률은 아직 높지 않은 것으로 나타났다. Thales가 전 세계 보안 전문가 2,767명을 대상으로 설문 조사를 진행한 결과, 제로 트러스트 도입을 적극적으로 수용 및 추진하고 있는 비율은 30%에 불과하였다[24]. 27%는 전략 개발을 수행하는 중이라고 답했으며, 나머지 43%는 도입할 계획이 없다고 답했다. 또한, Statista의 「제로 트러스트에 관한 통계 보고서」에 따르면, 제로 트러스트 보안 모델을 구현하여 제대로 시행

하고 있다고 응답한 비율은 31.7%에 불과하였으며, 나머지 68.3%는 Fig. 2와 같이 구현 계획이 없거나 시행에 어려움을 겪고 있는 것으로 나타났다[53].

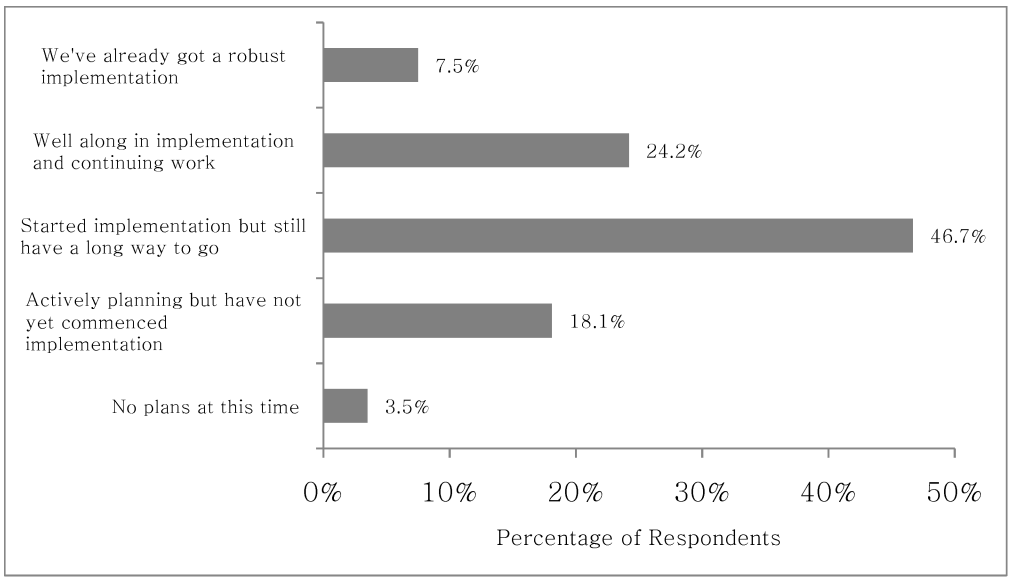

FIGURE 2. Graph of zero trust implementing status[53]

각국의 노력에도 불구하고 제로 트러스트 도입은 더딘 실정이다. 이는 제로 트러스트 도입을 방해하는 여러 가지 요인이 존재하기 때문이다. 전 세계 보안 전문가들은 제로 트러스트에 대한 지식 부족, 예산 부족, 기존 시스템과의 통합 문제 등을 제로 트러스트 도입을 위한 주요 과제로 꼽았다. 그중 가장 많은 응답자가 지적한 문제는 바로 애플리케이션의 서비스 응답 지연 시간 문제였다[53]. 제로 트러스트 아키텍처의 지속적인 사용자 신뢰도 평가와 모니터링으로 인해 지연 시간이 발생하는 것이다. 글로벌 보안 기업 Fortinet은 제로 트러스트를 성공적으로 확산시키기 위해서는 지연 시간이 짧은 제로 트러스트 솔루션을 구현하는 것이 중요하다고 지적

했다[54]. 그리고 미국 NIST도 접근 제어 절차 지연 시간은 워크플로우에 부정적인 영향을 미치므로 제로 트러스트 아키텍처의 성공적인 구현을 위해서는 지연 관리가 필수적이라고 주장했다[33]. 즉, 주요국의 제로 트러스트 정책이 성공적으로 이행되기 위해서는 초저지연 네트워크를 위한 제로 트러스트 아키텍처 개발이 뒷받침되어야 한다.

Ⅳ. 초저지연 네트워크 서비스 요구사항 분석

ITU(International Telecommunication Union)는 5G 무선 통신 기술의 핵심 서비스 유형을 URLLC(Ultra-Reliable Low-Latency Communication), mMTC(massive Machine Type Communications), eMBB(enhanced Mobile BroadBand)로 분류했다[55]. 이중 URLLC는 산업 자동화(Industry 4.0), 원격 수술, 자율주행자동차 등의 미션 크리티컬 애플리케이션과 실시간 애플리케이션을 지원하기 위해 가장 중요한 기능이다[56-58]. ITU에 따르면, URLLC 서비스에는 End-to-End 네트워크 지연 시간 제한이 필요하며[59], 3rd Generation Partnership Project(3GPP)는 URLLC를 위한 서비스 품질 요구사항으로 1ms의 대기 시간과 99.999%의 시스템 안전성을 요구한다[60]. 각 산업의 서비스 품질 요구사항을 살펴보면, 자동화 산업과 IoT 산업에서는 1ms의 종단 간 지연 시간이 요구된다[56, 61]. 자율주행 시스템은 10ms에서 100ms 사이의 지연 시간을 제공해야 하며, 안전을 위해 긴급 메시지 교환 지연 시간을 10ms 미만으로 유지해야 한다[62]. 원격 수술 시스템은 종단 간 지연 시간이 10ms 미만이어야 하며[63], 이외에 3GPP에서 제시한 5G 시스템 지연 시간 요구사항을 정리한 표는 TABLE Ⅰ과 같다. 5G 서비스 요구사항 분석 결과에 따르면 산업 시스템을 지원하기 위해서는 평균적으로 10ms 미만의 종단 간 지연 시간을 제공해야 한다[62].

TABLE I

Requirements for 5G system and network services[64]

Service	End-to-end requirement
Medical monitoring	< 100ms
Cloud/Edge rendering	< 5ms
Gaming/Interactive	< 10ms
Split control for robotics	< 12ms
Split AI/ML image recognition	< 2ms

Ⅴ. 관련 연구

다양한 산업에 제로 트러스트 기반 접근 제어 방식을 적용하고자 하는 연구가 진행되고 있다. 최근 관련 연구에서 각 산업의 특성을 반영하여 더욱 안전하고 효율적인 제로 트러스트 적용 방안을 제시했다. 본 장에서는 관련 연구를 통해 제로 트러스트 기반 접근 제어 방식 적용의 주요 과제를 분석한다. TABLE Ⅱ는 대표적인 관련 연구를 정리한 표이다.

TABLE Ⅱ

Previous studies on zero trust-based access control

Reference	Year	Proposed scheme	Limitation
Tyler and Viana[65]	2021	의료 산업에 적용할 수 있는 실용적인 제로 트러스트 솔루션	시스템 구축을 위해 다량의 방화벽 필요, 성능 부하
Chen et al[66]	2021	5G 스마트 헬스케어를 위한 제로 트러스트 기반 4차원 보안 프레임워크	높은 계산 비용, 지연 시간
Yang et al[67]	2021	제로 트러스트 기반 UAV 노드 인증 체계	성능 저하
Li et al[68]	2022	IoT를 위한 블록체인 기반 사용자 인증 방식	지연 시간
Wei and Yu[69]	2023	금융 시스템을 위한 머신러닝 기반 제로 트러스트 프레임워크	지연 시간

Tyler와 Viana는 의료 산업에 적용할 수 있는 실용적인 제로 트러스트 솔루션을 제시하였다. 의료 기관은 의료 기기 및 시스템상의 한계로 제로 트러스트 전환이 어렵다고 지적하면서, 방화벽, 프록시 서버 등의 레거시 시스템을 활용해 제로 트러스트를 구현할 수 있는 프레임워크를 개발 및 테스트했다. 낮은 지연 시간이 필수적인 의료 서비스를 고려하여 프록시 서버 대비 지연 시간 증가의 폭이 작은 방화벽을 마이크로 세그멘테이션에 이용했다. 그리고 단일 장애 지점 문제를 고려하여 네트워크 중복성을 보장하기 위한 방화벽 클러스터를 배치했다. 다만, 보조 방화벽으로 전환될 경우, 패킷 손실이 55% 발생했다. 해당 연구는 의료 산업을 위한 실용적인 제로 트러스트 프레임워크를 제시하고, 시뮬레이션을 통해 개념을 증명했다. 하지만, 마이크로 세그멘테이션 및 방화벽 클러스터 구축을 위해 수많은 방화벽이 필요하며, 이러한 방화벽은 성능 부하를 초래할 수 있다는 문제가 있다. 또한, 해당 프레임워크는 제로 트러스트의 핵심적인 요소인 사용자에 대한 엄격한 신뢰도 평가가 이루어지지 않는다[65].

Chen et al.은 전통적인 의료 서비스가 5G 기반의 애플리케이션으로 변화하면서 심각한 보안 및 개인정보 보호 문제에 직면했다고 지적하면서, 모든 사용자를 신뢰하지 않는 제로 트러스트가 5G 네트워크 보안에 적합한 방식이라고 설명했다. 본 연구에서는 제로 트러스트 기반의 5G 스마트 헬스케어를 위한 4차원 보안 프레임워크를 제안했고, 보안 차원을 주체, 개체, 환경, 행동으로 정의했다. 주체 및 환경을 중심으로 위험을 판단하는 메커니즘을 제시했으며, 주체 및 환경의 위험 수준을 평가하여 점수화하고 이를 기반으로 접근을 통제한다. 성능 평가를 통해 제안하는 프레임워크의 신뢰성, 안전성 등을 입증했으나, 지연 시간에 대한 평가는 이루어지지 않았다. 또한, 세션 수가 많아지면 인증 과정에서 높은 계산 비용과 자원 소모가 발생할 수 있다는 한계가 존재했다[66].

Yang et al.은 UAV(Unmanned Aerial Vehicle) 군집이 개방형 특성으로 인해 공격에 취약하며, 공격자는 신원을 위조하여 통신을 모니터링하거나 데이터를 변조할 수 있고 UAV 제어에 영향을 미칠 수 있다고 설명했다. 본 연구에서는 공격을 방지하기 위해 제로 트러스트 기반의 UAV 신원 인증 체계를 제안했다. UAV 마다 보안 게이트웨이를 설치하고, 보안 게이트웨이가 지상 관제소 및 다른 노드의 보안 게이트웨이와 통신하며 신원 인증을 수행한다. 구체적으로, UAV는 고유 UID와 Fingerprint, 원본 데이터를 암호화하여 자신의 보안 게이트웨이에 전송하고, 이를 수신한 보안 게이트웨이는 다른 UAV의 보안 게이트웨이로 데이터를 송신한다. 데이터를 수신한 다른 노드의 보안 게이트웨이는 자신의 UAV와 통신하며 신원을 인증한다. 본 연구에서는 이를 통해 공격을 신속하고 효과적으로 방지할 수 있다고 주장했다. 하지만, 제안한 인증 프로토콜이 UAV의 경량 요구사항을 충족할 수 있는지, 새로운 노드가 들어올 때 복잡한 인증 절차가 성능 저하를 초래하지 않는지에 대한 성능 평가는 이루어지지 않았다[67].

Li et al.은 5G/6G 기반의 IoT를 위한 제로 트러스트 보안 모델을 제안했다. IoT의 주요 보안 요구 사항으로 확장성과 높은 신뢰성, 낮은 에너지 소모량 등을 제시했으며, 특히 실시간 애플리케이션, 자동화된 산업 등을 위한 초저지연 보장이 중요하다고 분석했다. 제로 트러스트 모델은 5G-IoT에서 대부분의 보안 문제를 해결할 수 있지만, 각 장치의 지속적인 모니터링 및 분석과 활동 추적으로 인해 지연 시간을 유발한다는 문제가 있다고 지적했다. 본 연구에서는 제로 트러스트 접근 제어 방식에서 사용자를 검증하기 위한 블록체인 기반 IoT 장치 인증 방식을 제안했다. 이는 공개키 방식을 기반으로 디지털 서명을 생성하고, 이를 이용하여 신원증명을 수행한다. 하지만, 제안한 방식 역시 블록체인을 기반으로 디지털 서명을 생성하고 신원을 증명하는 과정에서 지연 시간이 유발되기 때문에 초저

지연 요구사항을 충족하기 어렵다[68].

Wei와 Yu는 디지털 금융 시스템을 안전하게 보호하기 위해 머신러닝(Machine Learning, ML) 기반의 제로 트러스트 모델을 제안하였다. ML 기반 제로 트러스트 프레임워크에서는 접근 요청이 발생하면 사용자의 정보를 수집한 뒤 ML을 통해 정보를 분석하여 사용자 신뢰도 평가를 수행하고, 그 결과를 바탕으로 접근 제어한다. 이러한 프레임워크는 높은 보안성을 제공할 수 있는 한편, ML을 활용한 사용자 신뢰도 평가 절차가 지연시간을 초래할 수 있다[69].

이처럼 디지털 산업에 제로 트러스트 기반 접근 제어 방식을 적용하고자 하는 연구가 활발히 진행되고 있으나, 대부분 보안 강화에 초점을 맞추고 있다. 제로 트러스트 적용으로 인한 성능 저하는 5G 초저지연 시대에서 중요한 문제이지만, 보안과 성능을 최적화하려는 시도는 거의 없었다.

Ⅵ. 저지연 고신뢰 클라우드 서비스를 위한 동적 제로 트러스트

1. 동적 제로 트러스트 개념

제로 트러스트 환경에서는 접근하는 클라우드 사용자의 신원과 행위, 정보 민감도, 환경 등을 종합적으로 평가하여 접근 요청을 처리한다[70]. 그러나, 접근 제어 과정에서 자원의 네트워크 요구사항이 고려되지 않으면, 지연 시간이 중요한 서비스의 경우에 제로 트러스트 아키텍처 적용이 제한될 수 있다[71]. 복잡한 사용자 신뢰도 평가 절차와 지속적인 모니터링 등이 지연 시간을 증가시키기 때문이다. 본 장에서는 성능과 보안을 최적화하는 DZTA(Dynamic Zero Trust Architecture)를 제안한다.

모든 접근 요청에 대해 Zero Trust 정책을 적용했던 종래의 방식과 달리, DZTA는 자원의 프라이버시 민감도 및 지연 민감도를 선제적으로 평가한 후, 그 결과에 따라 Zero Trust 정책, Conditional Trust 정책, Trust 정책을 동적으로 적용한다. Zero Trust 정책은 종래 방식과 마찬가지로 클라우드 사용자의 신원과 행위, 정보 민감도, 환경 등을 종합적으로 평가하여 접근 요청을 처리한다. Conditional Trust 정책은 클라우드 사용자의 신원만 인증하는 간소화된 절차가 적용된다. Trust 정책은 경계 기반 접근 제어 방식이 적용된 내부 네트워크처럼 별도의 사용자 신뢰도 평가 절차 없이 자원에 접근할 수 있도록 한다. 이러한 DZTA는 몇 가지 이점을 제공한다.

첫 번째는 보안과 성능을 최적화할 수 있다. DZTA는 자원의 프라이버시

민감도와 지연 민감도를 모두 평가하여 클라우드 접근 제어 정책을 결정하는 메커니즘으로써 보안과 성능 어느 하나에 치우치지 않고 최적화된 서비스를 제공할 수 있다.

두 번째는 미션 크리티컬 애플리케이션을 지원할 수 있다. 종래 제로 트러스트는 복잡한 사용자 신뢰도 평가 절차가 초래하는 지연 시간으로 인해 적용이 제한되는 서비스가 존재했는데, DZTA는 보안과 성능을 최적화하여 지연에 민감한 서비스의 요구사항을 충족시킬 수 있다.

2. 동적 제로 트러스트 구조와 동작 원리

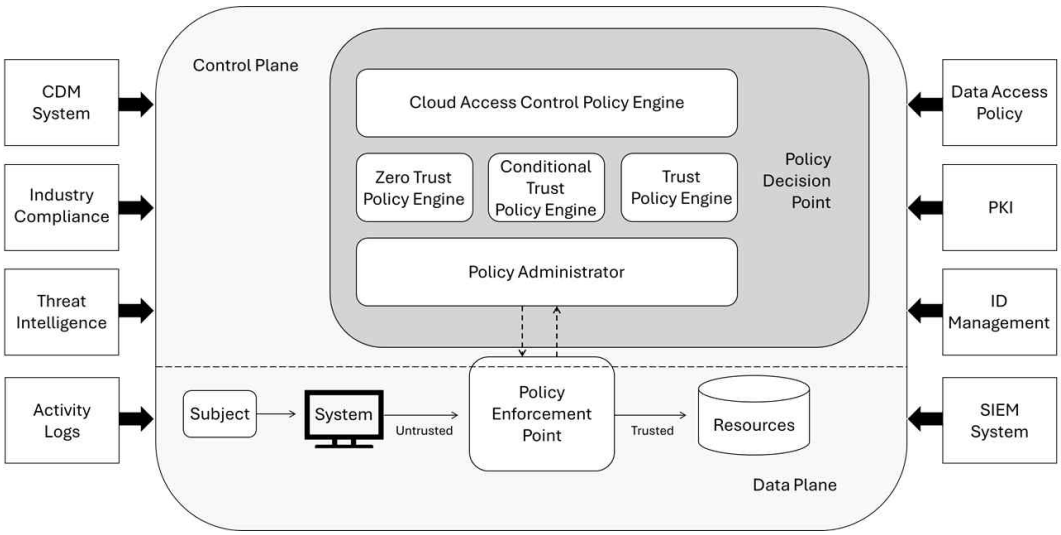

FIGURE 3. Dynamic zero trust architecture

Fig. 3은 본 논문에서 제안하는 DZTA이다. 클라우드 접근 제어 정책 엔진은 접근 대상의 프라이버시 민감도와 지연 민감도를 평가하여 적용할 정책을 결정하고, 결정 결과에 따라 Zero Trust 정책 엔진, Conditional

Trust 정책 엔진 또는 Trust 정책 엔진으로 접근 요청을 전달한다. Zero Trust 정책 엔진은 접근 요청을 전달받으면 접근하는 클라우드 사용자의 신원, 행위, 환경 등 다양한 제반 요소를 평가하여 접근 허용 여부를 결정한다. Conditional Trust 정책 엔진은 사용자 신뢰도 평가 절차를 간소화하여 접근하는 클라우드 사용자의 신원만 확인한 후 접근 여부를 결정하며, Trust 정책 엔진은 별도의 신뢰도 평가 절차 없이 자원 접근을 허용한다. 그리고 정책 관리자는 Zero Trust, Conditional Trust, Trust 정책 엔진의 결정 결과에 따라 인가 토큰을 발행하고, 정책 집행 지점과 통신하며 토큰을 전달한다. 정책 집행 지점은 정책 관리자와 통신하며 클라우드 사용자와 자원을 연결하거나 연결을 종료한다. 앞서 설명한 DZTA의 동작 과정을 정리하면 Fig. 4와 같다.

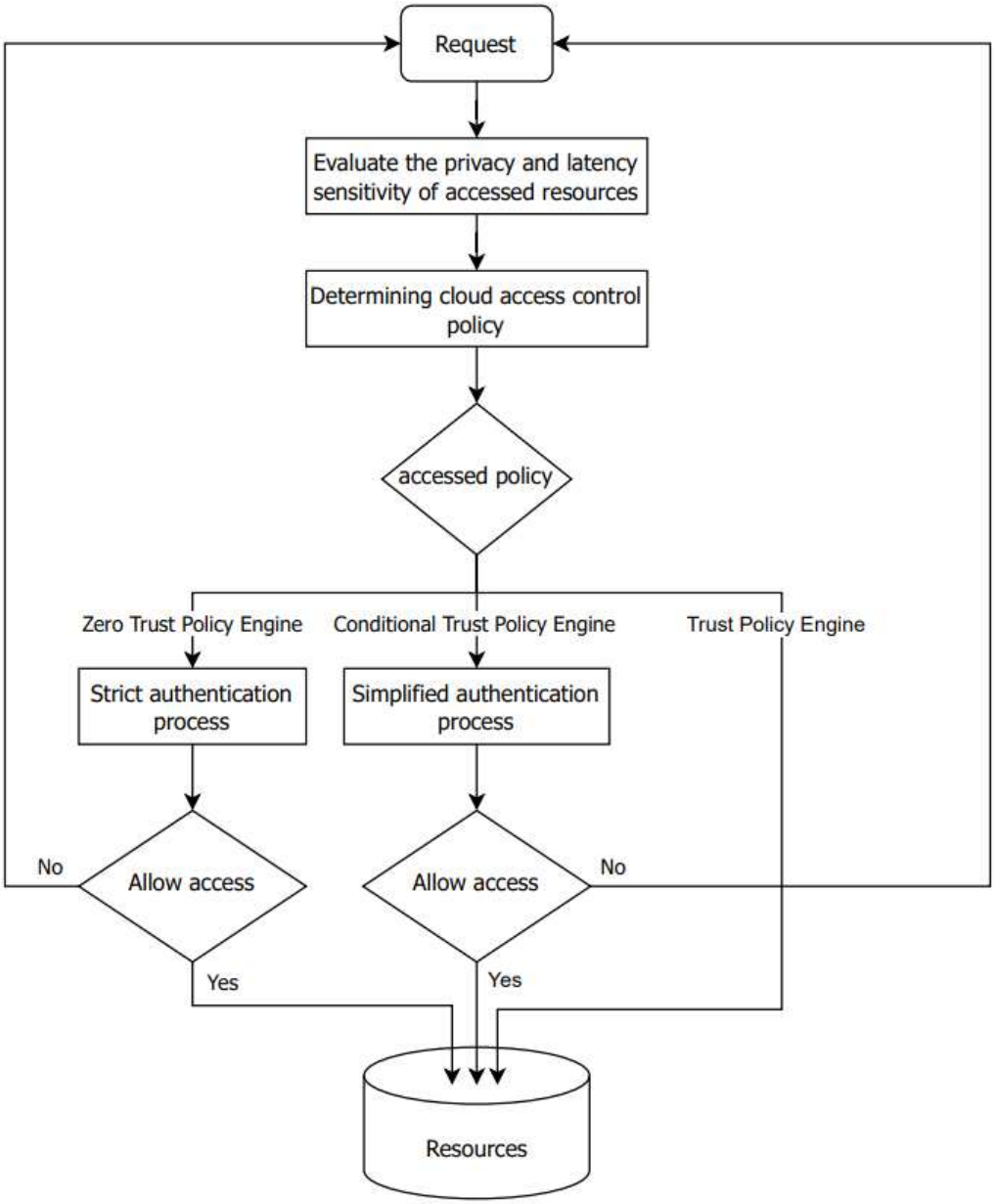

FIGURE 4. Flow chart of dynamic zero trust architecture

DZTA의 클라우드 접근 제어 정책 엔진에서 자원의 프라이버시 민감도와 지연 민감도를 검토한 후, 각각의 접근 요청에 대하여 어떠한 정책 엔

진에 포워딩할 것인지 결정하는 메트릭은 TABLE Ⅲ과 같다.

TABLE Ⅲ

Cloud access control policy engine decision metric

Data characteristics & Category		Cloud access control policy engine applied by data classification type
Privacy sensitivity	Latency sensitivity	
0	0	Trust Policy Engine
0	1	Trust Policy Engine
1	0	Zero Trust Policy Engine
1	1	Conditional Trust Policy Engine

오늘날 프라이버시 민감도에 따른 데이터 분류는 Public, Confidential, Restricted 등 3-5개 수준으로 분류하는 것이 일반적이다[72]. 마이크로소프트 Azure의 사례를 살펴보면, 기밀성에 따른 데이터 분류 체계를 Public, Internal, Confidential, Sensitive, Restricted로 구성하고 있으며, 데이터를 Confidential 이하와 Sensitive 두 개의 수준으로 분류하고, 각각 다른 접근 제어 정책을 적용하는 방식을 사용하여 개인정보를 보호하고 있다[73]. 본 연구에서도 프라이버시 민감도에 따라 자원을 두 가지 수준으로 이진 분류한다. 프라이버시에 민감한 데이터와 이를 이용하는 애플리케이션, 서비스 등은 민감한 자원으로 분류하고, 공개된 퍼블릭 데이터와 이를 이용하는 애플리케이션, 서비스 등은 퍼블릭 자원으로 분류한다. TABLE Ⅲ의 프라이버시 민감도 컬럼에서는 민감한 자원을 1, 퍼블릭 자원을 0으로 표현했다.

미션 크리티컬 애플리케이션과 애플리케이션에서 실시간 처리를 요구하는 데이터는 지연에 민감한 자원으로 분류할 수 있다[74]. 애플리케이션 및 데이터의 유형에 따라 QoS(Quality of Service) 요구사항은 모두 다르며, 우선순위 수준을 기반으로 자원을 분류할 수 있다. 한 연구에서는 QoS를 기반으로 데이터를 적시성이 높은 데이터, 적시성이 낮은 데이터, 주기적 데이터 세 가지 범주로 분류했다[75]. 본 연구에서는 지연 민감도에 따라 데이터를 이진 분류하며, Table Ⅲ의 지연 민감도 컬럼에서 지연 시간에 민감한 자원은 1, 그렇지 않은 자원은 0으로 표현했다.

클라우드 접근 제어 정책 결정 메트릭에서 퍼블릭 자원의 경우, 지연 민감도와 관계없이 모두 Trust 정책 엔진으로 포워딩한다. 하지만, 프라이버시에 민감한 자원은 지연 민감도에 따라 포워딩 되는 정책 엔진이 달라진다. 지연 시간에 민감한 자원의 경우 간소화된 사용자 신뢰도 평가 절차를 적용하는 Conditional Trust 정책 엔진에 포워딩하고, 그렇지 않으면 엄격하게 사용자의 신뢰도를 평가하는 Zero Trust 정책 엔진으로 포워딩한다.

Ⅶ. 성능 평가와 분석

1. 평가 모델

본 논문에서는 제안하는 DZTA가 보안과 성능을 최적화할 수 있음을 입증하기 위해 클라우드 접근 제어 정책의 효과를 수학적으로 모델링했다. 모델링한 수식을 바탕으로 경계 기반 접근 제어 방식, ZTA, DZTA의 보안과 성능에 대한 수치 분석 결괏값을 구하고 비교 분석을 통해 효과를 입증한다.

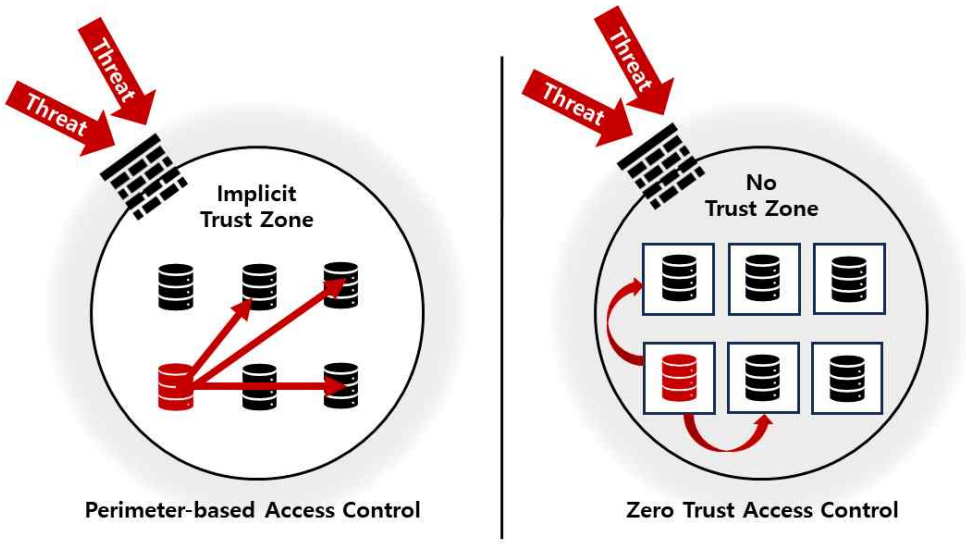

FIGURE 5. Comparison of perimeter-based access control and zero trust access control[76]

경계 기반 접근 제어 방식과 ZTA, DZTA가 가장 큰 차이를 보이는 지

점은 내부 네트워크에서의 접근 제어 방식이다. Fig. 5와 같이 경계 기반 접근 제어 방식은 내부 사용자에게 암시적 신뢰를 부여하는 반면, 제로 트러스트 보안은 누구에게도 신뢰를 부여하지 않는다. 수치 분석에서는 이러한 차이를 확인하기 위해 사용자가 내부 네트워크에 있는 경우를 상정한다. 따라서, 경계 보안 방식은 추가 인증 없이 자유롭게 모든 자원에 접근할 수 있고, ZTA와 DZTA는 각 세그먼트에 접근할 때마다 접근 제어 정책이 적용된다. 또한, 본 연구에서는 ZTA와 DZTA 모두 개별 자원 단위로 마이크로 세그멘테이션한 환경을 가정한다. TABLE Ⅳ는 수학적 모델링에 사용한 파라미터의 정보이다.

TABLE Ⅳ

Performance evaluation parameters

Parameter	Description
n_{ds}	Number of data sources
n_c	Number of one-way communications among internal components
n_{ZT}	Number of segments with zero trust policy engine applied
n_{CT}	Number of segments with conditional trust policy engine applied
n_T	Number of segments with trust policy engine applied
R	Number of resources
r_n	Number of resources in the n^{th} segment
ps_n	Resource privacy sensitivity of the n^{th} segment
p	Probability of successful attack
L_{E2E}	End-to-end latency
L_{ZT-E2E}	End-to-end latency when applying the zero trust policy
L_{CT-E2E}	End-to-end latency when applying the conditional trust policy
L_{T-E2E}	End-to-end latency when applying the trust policy
$L_{one-way}$	One-way communication latency
L_{Avg}	Average end-to-end latency for dynamic zero trust architecture

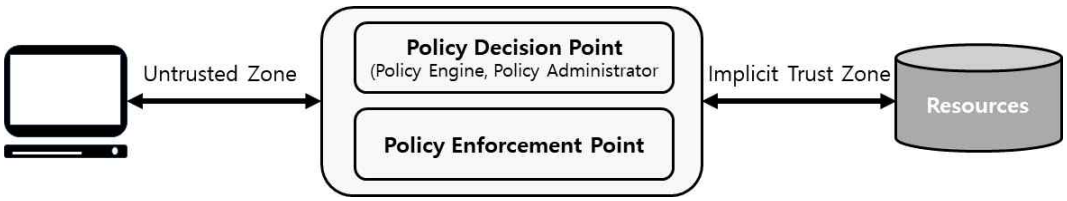

FIGURE 6. Zero trust access process[33]

Fig. 6은 ZTA가 자원에 대한 접근 요청을 처리하는 과정을 표현한 그림이다. 사용자의 접근 요청은 여러 내부 컴포넌트를 거쳐 정책 엔진에 도달하며, 정책 엔진은 데이터 소스들로부터 정보를 수집하여 사용자의 신뢰도를 평가한다. 정책 엔진이 접근 여부를 결정하면 그 결과는 다시 여러 컴포넌트를 거쳐 사용자에게 전달되며, 접근을 허용한 경우 사용자는 세그먼트 내의 자원에 접근할 수 있다[33]. 따라서, ZTA의 종단 간 지연 시간은 내부 컴포넌트 간 통신에서 발생하는 지연 시간과 정책 엔진이 외부 데이터 소스에서 정보를 수신할 때 발생하는 지연 시간을 더하여 구할 수 있으며, 수식(1)로 모델링된다.

$$L_{EET} = L_{one-way} \times (n_c + 2 \times n_{ds}) \quad (1)$$

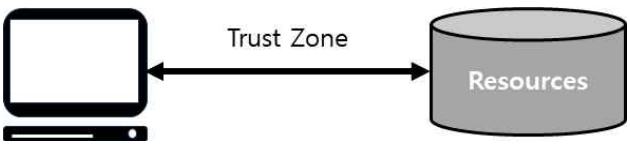

FIGURE 7. Perimeter-based access process

경계 기반 접근 제어 방식은 내부 네트워크에 암시적 신뢰를 부여하므로

추가 인증 절차 없이 자원에 접근할 수 있으며[77], 이를 그림으로 표현하면 Fig. 7과 같다. 따라서, 경계 기반 접근 제어 방식의 종단 간 지연 시간은 자원 요청 및 응답의 양방향 통신에 대해서만 발생하며, 수식(2)로 모델링된다.

$$L_{E2E} = L_{one-way} \times 2 \tag{2}$$

DZTA도 ZTA와 마찬가지로 내부 컴포넌트 간 통신을 통해 접근 요청과 요청 처리 결과를 주고받으며, 클라우드 사용자의 신뢰도를 평가하기 위해 외부 데이터 소스들과의 양방향 통신을 수행한다. 다만, DZTA는 클라우드 접근 제어 정책 엔진이 Zero Trust 정책 엔진 또는 Conditional Trust 정책 엔진 또는 Trust 정책 엔진으로 접근 요청을 포워딩하는 단방향 통신이 추가로 존재한다. 또한, DZTA는 정책마다 사용자 신뢰도 평가 절차가 달라서 각 정책 엔진과 데이터 소스 간 통신 횟수가 다르다. Zero Trust 정책 엔진의 경우 데이터 소스 수만큼 양방향 통신이 발생하며, Conditional Trust 정책 엔진은 사용자 신원증명을 수행하는 데이터 소스와의 양방향 통신만 발생한다. Trust 정책 엔진은 데이터 소스에서 정보를 수신하지 않으므로 통신이 발생하지 않는다. 이처럼 DZTA는 각 정책 엔진마다 데이터 소스와의 통신 횟수(n_{ds})가 다르므로 종단 간 지연 시간도 다르다. 본 수치 분석에서는 Zero Trust, Conditional Trust, Trust 정책 엔진에서 발생하는 지연 시간을 모두 반영하기 위해 평균 종단 간 지연 시간을 산출한다. 평균 종단 간 지연 시간을 구하는 방법은 다음과 같다. ① Zero Trust, Conditional Trust, Trust 정책 엔진 각각의 종단 간 지연 시간과 각 정책이 적용되는 자원의 수를 곱한 다음 그 결과들을 모두 합한다. ② 1번의 결과를 총자원 수로 나누면 한 자원에 접근할 때 발생하는

평균 종단 간 지연 시간이 도출된다. 평균 종단 간 지연 시간을 수식으로 표현하면 다음과 같다:

$$L_{Avg} = \frac{(n_{ZT} \times L_{ZT-ETT} + n_{CT} \times L_{CT-ETT} + n_T \times L_{T-ETT})}{R} \quad (3)$$

수식(3)에서 L_{ZT-ETT}는 Zero Trust 정책 엔진이 적용될 때 발생하는 종단 간 지연 시간을 의미하며 수식(2)를 통해 구할 수 있고, L_{CT-ETT}는 Conditional Trust 정책 엔진에 대한 종단 간 지연 시간으로서 L_{ZT-ETT}와 마찬가지로 수식(2)를 통해 구할 수 있으며, L_{T-ETT}는 Trust 정책 엔진의 종단 간 지연 시간을 의미하며 수식(4)를 통해 구할 수 있다.

$$L_{T-ETT} = L_{one-way} \times n_c \quad (4)$$

제안한 방식과 종래 방식의 보안성은 각 아키텍처의 공격 파급력을 계산하여 평가하였다. 공격은 자원에 대한 비인가 접근 시도를 의미한다. 공격 파급력은 각 세그먼트에 대한 공격 성공 확률과 해당 세그먼트에 저장되어 있는 자원 수, 자원의 프라이버시 민감도 수준을 곱한 뒤, 전체 세그먼트의 계산 결과를 모두 더하여 구할 수 있다. 프라이버시 민감도 수준을 곱하는 이유는 퍼블릭 자원의 경우 기이 공개된 것이므로 유출이 되더라도 영향을 미치지 않기 때문이다. 경계 기반 접근 제어 방식과 ZTA, DZTA는 자원 접근 제어 방식에 차이가 있어서 공격의 난이도가 모두 다른데, 이를 반영하기 위해 공격 성공 확률에 데이터 소스의 수를 거듭제곱한다. 정보를 제공하는 데이터 소스의 수가 많을수록 공격이 어려워지는 현상을 반영하기 위함이다. 본 수치 분석에서 데이터 소스의 수는 8개로 설정하였고, DZTA

의 Conditional Trust 정책은 사용자의 신원을 확인하는 데이터 소스 1개만 활용한다. Trust 정책은 사용자 신뢰도 평가 절차가 없어서 데이터 소스에서 정보를 수신하지 않는다. 먼저, ZTA와 DZTA의 공격 파급력(IoA_Z)을 구하는 수식은 다음과 같다:

$$IoA_Z = \sum_{n=1}^{R} p^{n_{ds}} \times r_n \times ps_n \quad (5)$$

제로 트러스트 아키텍처의 공격 파급력은 수식(5)를 통해 구할 수 있다. 개별 자원 단위로 마이크로 세그멘테이션하므로 세그먼트의 수는 자원 수와 동일하며, r_n은 모두 1이다. 또한, 사용자의 신뢰도를 평가할 때 모든 데이터 소스로부터 정보를 수집하므로 데이터 소스의 수(n_{ds})는 항상 8이다.

동적 제로 트러스트 아키텍처의 공격 파급력도 수식(5)를 통해 구할 수 있다. DZTA는 정책마다 사용자 신뢰도 평가 절차가 다른데, Zero Trust 정책은 사용자의 신뢰도를 평가할 때 모든 데이터 소스로부터 정보를 수신하므로 n_{ds}가 8이고, Conditional Trust 정책은 사용자 신원을 확인하는 데이터 소스에서만 정보를 수신하므로 n_{ds}가 1이다. Trust 정책은 사용자 신뢰도 평가 절차가 없어서 데이터 소스로부터 정보를 수신하지 않으므로 n_{ds}는 0이다.

경계 기반 접근 제어 방식은 마이크로 세그멘테이션을 하지 않으므로 전체 세그먼트의 수가 하나이고, 세그먼트 내의 자원 수는 전체 자원의 수와 같다. 또한, 사용자 신뢰도 평가 절차가 없어서 데이터 소스에서 정보를 수신하지 않으므로 데이터 소스의 수는 0이며, 퍼블릭 자원은 유출이 되더라

도 영향을 미치지 않으므로 프라이버시 민감도가 높은 자원만 고려하여 계산한다. 이러한 특성을 수식(5)에 반영하여 정리한 경계 기반 접근 제어 방식의 공격 파급력(IoA_P)은 수식(6)과 같다:

$$IoA_P = p^0 \times \mathrm{Pr}ivacy\ \ Sensitive\ \ Resources \tag{6}$$

2. 평가 결과와 분석

전체 자원 중 지연 민감도가 큰 자원과 프라이버시 민감도가 큰 자원의 비율을 조정하며 각 아키텍처의 종단 간 지연 시간과 공격 파급력을 비교하였다. 이때, 단방향 통신 지연 시간 $L_{one-way}$는 현재 5G NR 시스템의 단방향 지연 시간을 고려하여 0.5ms로 설정하였다[62, 78-80]. 수치 분석에 사용한 파라미터는 TABLE Ⅴ와 같다.

TABLE Ⅴ

Value of performance evaluation parameters

Parameter	Value
$L_{one-way}$	0.5ms
R	50
p	0.05

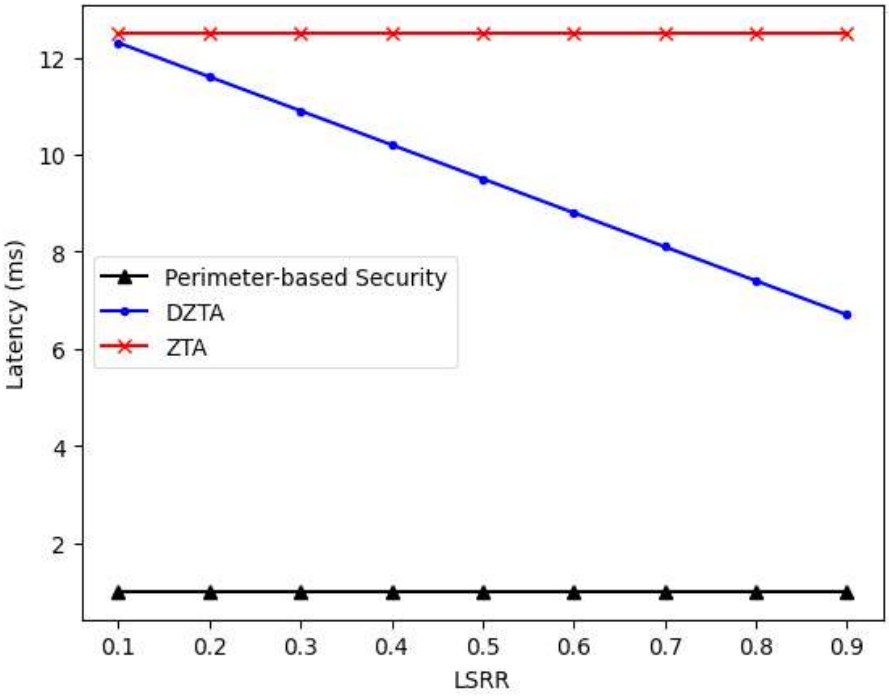

FIGURE 8. Latency by LSRR

Fig. 8은 LSRR(Latency Sensitive Resources Ratio)에 따른 각 아키텍처의 평균 종단 간 지연 시간을 나타낸 그래프이다. LSRR은 지연에 민감한 자원의 수를 전체 자원 수로 나눈 값으로, 수식으로 표현하면 수식(7)과 같다. 프라이버시 민감도는 모두 1로 고정하였다.

$$LSRR = \frac{Number\ of\ latency\ sensitive\ data}{R} \tag{7}$$

경계 기반 접근 제어 방식은 내부 네트워크에서 인증 절차 없이 자원에 접근할 수 있으므로 자원 접근 요청 및 응답 지연 시간만 일정하게 발생하

였다. 그리고 ZTA와 DZTA의 종단 간 지연 시간은 정보를 수신하는 데이터 소스의 수 n_{ds}와 내부 컴포넌트 간 단방향 통신 횟수 n_c에 따라 차이가 발생한다. ZTA는 지연 민감도를 고려하지 않으므로 지연에 민감한 자원의 비율과 관계없이 매 접근마다 모든 데이터 소스로부터 정보를 수신하기 때문에 10ms 이상의 종단 간 지연 시간이 일정하게 발생하였다. 반면에 DZTA는 지연에 민감한 자원에 대한 접근 요청이 들어올 경우, 사용자 신뢰도 평가 절차가 간소화된 Conditional Trust 정책이 적용되므로 지연에 민감한 자원의 비율이 높아질수록 평균 지연 시간이 감소했다. 내부 컴포넌트 간 단방향 통신 횟수는 DZTA가 1회 더 많으나, 미미한 수준이어서 전체 지연 시간에 큰 영향을 미치지 않는다.

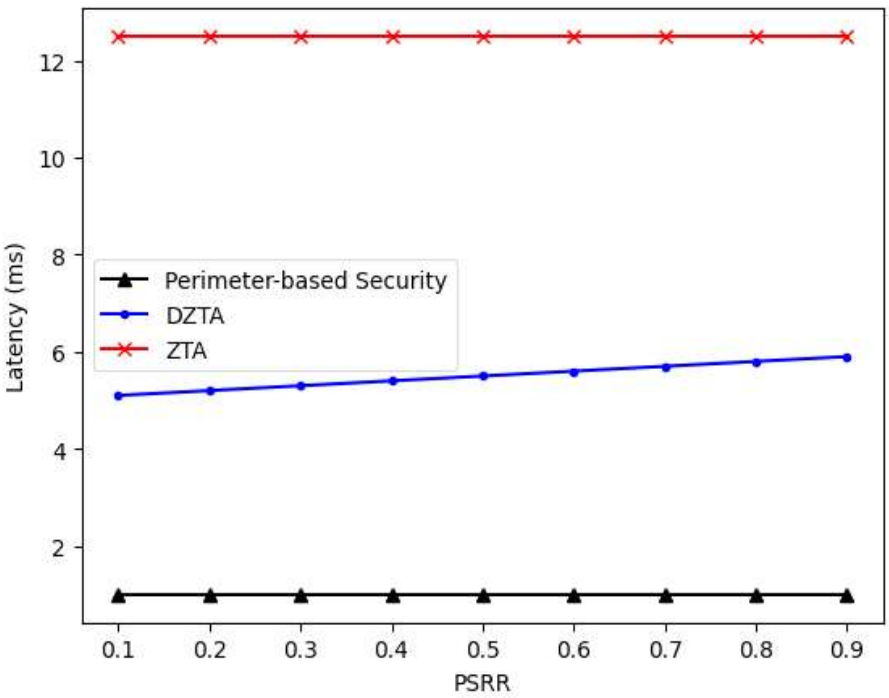

FIGURE 9. Latency by PSRR

Fig. 9는 지연 민감도를 모두 1로 고정하고 PSRR(Privacy Sensitive Resources Ratio)을 조정하며 각 아키텍처의 종단 간 지연 시간을 측정한 그래프이다. PSRR을 수식으로 표현하면 수식(8)과 같다.

$$PSRR = \frac{Number\,of\,privacy\,sensitive\,data}{R} \tag{8}$$

경계 기반 접근 제어 방식은 자원 접근 요청 및 응답의 양방향 통신 지연 시간만 일정하게 발생하였고, ZTA는 사용자의 신뢰를 평가할 때 매번 모든 데이터 소스와 통신하므로 10ms 이상의 지연 시간이 일정하게 발생하였다. 반면에 DZTA는 프라이버시 민감도에 따라 Conditional Trust 또는 Trust 정책이 동적으로 적용되므로 ZTA에 비해 평균 종단 간 지연 시간이 낮았다. 다만, 프라이버시에 민감한 자원의 수가 증가할수록 사용자 신뢰도 평가를 수행하는 자원이 늘어나므로 평균 종단 간 지연 시간이 점진적으로 증가했다.

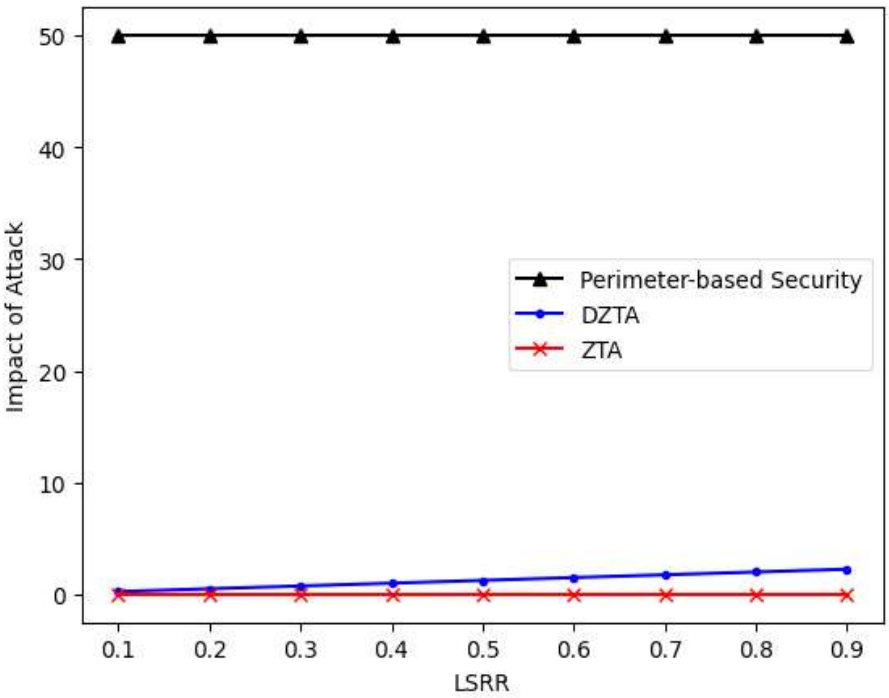

FIGURE 10. Impact of attack by LSRR

Fig. 10은 LSRR에 따른 공격 파급력을 나타낸 그래프이다. 공격 파급력에 큰 영향을 미치는 요소는 마이크로 세그멘테이션 여부와 파라미터 n_{ds}이며, 데이터 소스의 수(n_{ds})가 많을수록 공격 성공 확률은 지수적으로 감소한다. 경계 기반 접근 제어 방식은 마이크로 세그멘테이션을 하지 않으며, 사용자 신뢰도 평가 절차가 없기 때문에 공격 파급력이 매우 컸다. 반면, ZTA와 DZTA는 0에 가까운 매우 낮은 공격 파급력을 가졌다. DZTA는 지연에 민감한 자원이 많을수록 공격 파급력이 증가했는데, 이는 지연에 민감한 자원의 비율이 높아질수록 간소화된 사용자 신뢰도 평가 절차가 적용되는 자원이 늘어나기 때문이다.

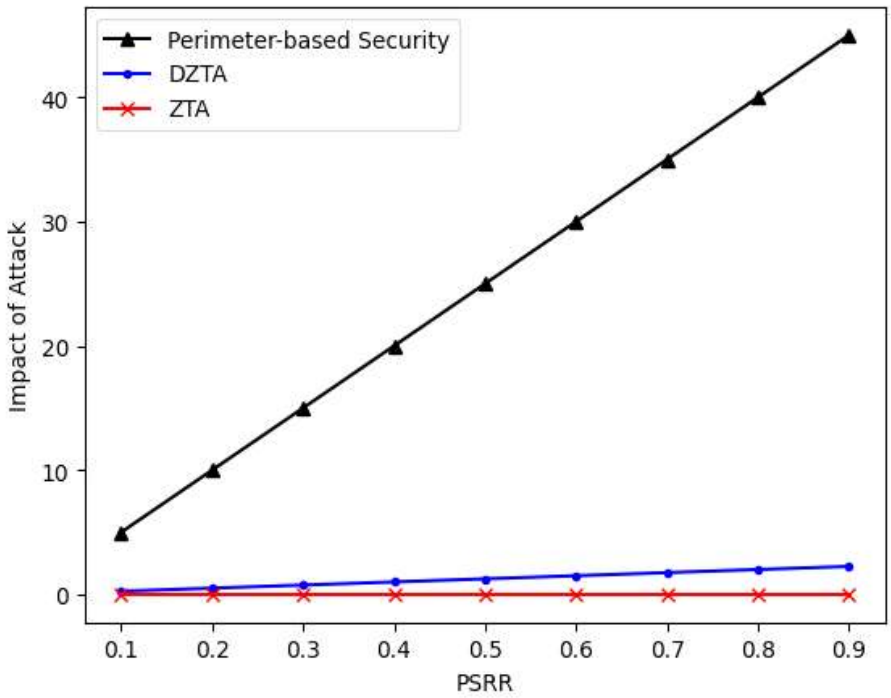

FIGURE 11. Impact of attack by PSRR

Fig. 11은 PSRR에 따른 각 아키텍처의 공격 파급력을 비교한 그래프이다. 프라이버시 민감도가 낮은 퍼블릭 데이터는 유출이 되더라도 영향을 미치지 않기 때문에 프라이버시에 민감한 데이터의 비율이 높아질수록 공격 파급력이 증가하였다. 경계 기반 접근 제어 방식은 프라이버시에 민감한 데이터의 비율이 커질수록 공격 파급력이 큰 폭으로 증가하였으며, ZTA와 DZTA는 0에 가까운 낮은 값을 유지하였다.

Ⅷ. 기대효과

1. 보안과 성능 최적화

레거시 ZTA는 보안에 초점을 맞춘 모델로, 자원의 지연 민감도를 고려하지 못하고 있다. 하지만, 디지털화된 사회에서는 보안과 성능을 모두 제공하는 것이 필수적이며, 특히 자율주행자동차, 의료 서비스, 자동화된 산업 등의 미션 크리티컬 애플리케이션은 초저지연 요구사항을 반드시 충족해야 한다. DZTA는 레거시 ZTA의 한계점을 개선한 모델로, 지연 민감도와 프라이버시 민감도를 평가하여 자원을 분류하는 컴포넌트를 추가함으로써 각 자원에 적합한 클라우드 접근 제어 정책을 동적으로 적용할 수 있도록 설계하였다. 따라서, 프라이버시 민감도가 낮은 자원은 신속하게 접근하고 이용할 수 있고, 프라이버시 민감도와 지연 민감도가 모두 큰 자원은 간소화된 사용자 신뢰도 평가 절차를 적용하여 보안과 성능을 동시에 보장할 수 있다. 본 연구에서는 수치 분석을 기반으로 한 성능 평가를 통해 경계 기반 접근 제어 방식과 ZTA, DZTA의 지연 시간 및 공격 파급력을 비교하였고, DZTA가 두 가지 평가 지표에서 모두 좋은 성능을 보이며 보안과 성능을 최적화할 수 있음을 입증했다.

2. 저지연 서비스 지원

Ⅳ장에서 초저지연 네트워크 서비스 요구사항을 분석한 결과에 따르면, 저지연 서비스를 지원하기 위해서는 10ms 이하의 지연 시간을 보장할 수

있어야 한다. 하지만, ZTA의 복잡하고 지속적인 사용자 신뢰도 평가 절차는 지연 시간을 초래하여 저지연 서비스로의 적용을 어렵게 한다. 반면, DZTA는 지연에 민감한 서비스에 대해 신속한 사용자 신뢰도 평가 절차를 지원하기 때문에 저지연 서비스에서도 효과적인 활용이 가능하다. 성능 평가 결과에 따르면 ZTA는 10ms 이상의 지연 시간이 발생했지만, DZTA는 평균 10ms 이하의 지연 시간을 유지했다. 그뿐만 아니라 지연 민감도가 높은 자원의 비율이 높을수록 평균 지연 시간은 더욱 감소했다.

3. 주요국의 제로 트러스트 클라우드 접근 제어 정책 실현

Ⅲ장에서 분석한 바와 같이, 주요국은 제로 트러스트 접근 제어 정책을 사이버 보안의 핵심 전략으로 채택하고 이에 대한 투자를 확대해 나가고 있다. 특히 미국은 정부 시스템에 제로 트러스트 도입을 의무화하는 등 강력한 정책을 시행하고 있으며, 공공 부문을 시작으로 제로 트러스트 적용 전략을 민간으로 확대해 나갈 것으로 전망된다. 하지만, 제로 트러스트의 지연 시간 문제는 클라우드 산업 현장에 제로 트러스트 접근 제어 정책을 적용할 때 큰 걸림돌이 될 수 있으며, 특히 저지연 서비스를 제공하는 기관은 정책 이행에 차질을 빚을 수 있다. DZTA는 보안과 성능을 모두 보장하므로 이러한 어려움을 해소할 수 있다. DZTA는 레거시 ZTA 대비 여러 산업의 요구사항을 충족할 수 있어서 각국의 제로 트러스트 정책 실현을 효과적으로 뒷받침할 수 있다.

Ⅸ. 결론 및 향후 연구

본 연구에서는 저지연 서비스를 지원하기 위한 DZTA를 제안했다. 후속 연구에서는 DZTA를 모델링하고 시뮬레이션을 수행하여 실제 산업에서 활용 가능함을 입증할 예정이다. 제로 트러스트 접근 제어 방식은 미래 융합 산업의 유망한 기술로 주목받고 있지만, 지연 시간 등의 주요 과제가 남아 있다. 따라서, 제로 트러스트 접근 제어 방식이 다양한 산업에 적용될 수 있도록 보안과 성능을 모두 보장하는 DZTA를 제안하였다. 종래 ZTA에 클라우드 접근 제어 정책을 동적으로 적용하는 컴포넌트를 추가함으로써 DZTA는 지연 시간 문제를 해소하고, 보안과 성능을 동시에 보장할 수 있다.

참 고 문 헌

[1] Lambropoulos, G., Mitropoulos, S. and Douligeris, C., 2021. A Review on Cloud Computing services, concerns, and security risk awareness in the context of Digital Transformation. 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Preveza, Greece, pp. 1-6.

[2] Wu, J. C., Lee, S. M., & Chen, C. J. (2023, May). Exploring the Context with Factors of Cloud Computing to Digital Transformation and Innovation. In International Conference on Knowledge Management in Organizations (pp. 115-136). Cham: Springer Nature Switzerland.

[3] Mydyti, H., Ajdari, J., Zenuni, X., 2020. Cloud-based Services Approach as Accelerator in Empowering Digital Transformation. In 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), pp. 1390-1396, IEEE.

[4] El-Haddadeh, R., 2020. Digital innovation dynamics influence on organisational adoption: the case of cloud computing services. Information Systems Frontiers, vol. 22, no. 4, pp. 985-999.

[5] Nanos, I., Manthou, V., & Androutsou, E., 2019. Cloud computing adoption decision in E-government. In Operational Research in the Digital Era-ICT Challenges: 6th International Symposium and 28th National Conference on Operational Research, Thessaloniki, Greece,

pp. 125-145. Springer International Publishing.

[6] Adjei, J. K., Adams, S., & Mamattah, L., 2021. Cloud computing adoption in Ghana; accounting for institutional factors. Technology in Society, vol. 65, 101583.

[7] Liang, Y., Qi, G., Zhang, X., & Li, G., 2019. The effects of e-Government cloud assimilation on public value creation: An empirical study of China. Government Information Quarterly, vol. 36, no. 4, 101397.

[8] Statista Research Department, 2023. Revenue of the public cloud industry worldwide 2019-2028.

[9] Patel, A., Shah, N., Ramoliya, D., & Nayak, A., 2020. A detailed review of Cloud Security: Issues, Threats & Attacks. 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 758-764.

[10] Aparajit, S., Shah, R., Chopdekar, R. & Patil, R., 2022. Data Protection: The Cloud Security Perspective. 2022 3rd International Conference for Emerging Technology (INCET), Belgaum, India, pp. 1-5.

[11] Doshi, R. & Kute, V., 2020. A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models. 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, pp. 1-4

[12] Kumar, R., & Goyal, R., 2019. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, vol. 33, pp. 1-48.

[13] Hu, V. C., Iorga, M., Bao, W., Li, A., Li, Q., & Gouglidis, A., 2020. General access control guidance for cloud systems. NIST Special Publication 800-210, 50-2ex.

[14] Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y., 2019. Survey of access control models and technologies for cloud computing. Cluster Computing, vol. 22, pp. 6111-6122.

[15] John, J., & Norman, J., 2019. Major vulnerabilities and their prevention methods in cloud computing. In Advances in Big Data and Cloud Computing: Proceedings of ICBDCC18 (pp. 11-26). Springer Singapore.

[16] Kholidy, H. A., Karam, A., Sidoran, J., Rahman, M. A., Mahmoud, M., Badr, M., Mahmud, M. and Sayed, A. F., 2022. Toward Zero Trust Security IN 5G Open Architecture Network Slices. 2022 IEEE Military Communications Conference (MILCOM), Rockville, MD, USA, pp. 577-582.

[17] Alalmaie, A. Z., Nanda, P., He, X., Alayan, M. S., 2023. Why Zero Trust Framework Adoption has Emerged During and After Covid-19 Pandemic. International Conference on Advanced Information Networking and Applications, Cham: Springer International Publishing, pp. 181-192.

[18] Bobbert, Y., & Scheerder, J., 2022. Zero Trust Validation: from Practice to Theory: An empirical research project to improve Zero Trust implementations. In 2022 IEEE 29th Annual Software Technology Conference (STC), pp. 93-104. IEEE.

[19] Phiayura, P., & Teerakanok, S., 2023. A Comprehensive Framework

for Migrating to Zero Trust Architecture. IEEE Access, vol. 11, pp. 19487-19511.

[20] Federici, F., Martintoni, D., & Senni, V., 2023. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. Electronics, vol. 12, no. 3.

[21] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig Z. and Doss, R., 2022. Zero Trust Architecture (ZTA): A Comprehensive Survey. in IEEE Access, vol. 10, pp. 57143-57179.

[22] Mehraj, S., & Banday, M. T., 2020. Establishing a zero trust strategy in cloud computing environment. In 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6. IEEE.

[23] Mehraj, S. and Banday, M. T., 2020. Establishing a Zero Trust Strategy in Cloud Computing Environment. 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-6.

[24] THALES, Navigating Data Security in an Era of Hybrid Work, Ransomware and Accelerated Cloud Transformation, 2022 Thales Data Threat Report: Global Edition, 2022.

[25] Yiliyaer, S., Kim, Y., 2022. Secure Access Service Edge: A Zero Trust Based Framework For Accessing Data Securely. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 0586-0591.

[26] Sengupta, B., Lakshminarayanan, A., 2021. Distritrust: Distributed and low-latency access validation in zero-trust architecture. Journal

of Information Security and Applications, vol. 63.

[27] Liu, Y., Deng, Y., Nallanathan, A. and Yuan, J., 2023. Machine Learning for 6G Enhanced Ultra-Reliable and Low-Latency Services. in IEEE Wireless Communications, vol. 30, no. 2, pp. 48-54.

[28] Li, S., Iqbal, M., Saxena, N., 2022. Future Industry Internet of Things with Zero-trust Security. Information System Fronttiers.

[29] Lin, Y., Lin, L., 2019. Design and Realization of a Computer Security Control Circuit for Local Area Network. 2019 International Conference on Communications, Information System and Computer Engineering (CISCE), Haikou, China, pp. 9-12.

[30] Capmbell, M., 2020. Beyond Zero Trust: Trust Is a Vulnerability. Computer, vol. 53. no. 10, pp. 110-113.

[31] Kindervag, J., Balaouras, S., Coit, L., 2010. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. for Security & Risk Professionals, pp. 1-25.

[32] Kang, H., Liu, B., Mišić, J., Mišić, V. B., & Chang, X., 2020. Assessing Security and Dependability of a Network System Susceptible to Lateral Movement Attacks, 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, pp. 513-517

[33] Stafford, V. A. (2020). Zero trust architecture. NIST special publication 800-207.

[34] The White House, 2021. Improving the Nation's Cybersecurity, Executive Order 14028 of May 12, 2021. Federal Register, vol. 86, no. 93.

[35] Cybersecurity and Infrastructure Security Agency(CISA), 2021. Zero Trust Maturity Model Version 1.0.

[36] Office of Management and Budget(OMB), 2022. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. M-22-09 Memorandum for the head of executive departments and agencies, Jan. 2022.

[37] National Institute of Standards and Technology(NIST), 2022. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators

[38] National Institute of Standards and Technology(NIST), 2022. Implenting a Zero Trust Architecture. NIST Special Publication 1800-35A, vol. A.

[39] National Institute of Standards and Technology(NIST), 2023. Implenting a Zero Trust Architecture. NIST Special Publication 1800-35B, vol. B.

[40] National Institute of Standards and Technology(NIST), 2023. Implenting a Zero Trust Architecture. NIST Special Publication 1800-35C, vol. C.

[41] National Institute of Standards and Technology(NIST), 2022. Implenting a Zero Trust Architecture. NIST Special Publication 1800-35D, vol. D.

[42] U.S. Department of State, 2023. Congressional Budget Justification Department of State, Foreign Operations, and Related Programs. FISCAL YEAR 2024.

[43] European Union, 2022. Measures for a high common level of

cybersecurity across the Union. Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS 2 Directive).

[44] European Commission, 2022. ENsuring Secure and Safe CMD Design with Zero TRUST Principles. https://cordis.europa.eu/project/id/101095634.

[45] Presidential Committee on the Digital Platform Government, 2023. Digital Platform Government Realization Plan.

[46] Ministry of Science and ICT, Korea Internet & Security Agency, Korea Zero Trust Alliance, 2023. Zero Trust Guideline 1.0.

[47] Ministry of Science and ICT, Korea Internet & Security Agency, 2023. Zero Trust Security Model Demonstration Support Project Conspire, Ministry of Science and ICT Announcement No. 2023-0491.

[48] Digital Agency Government of Japan, 2021. Focus plan for the realization of a digital society.

[49] Digital Agency Government of Japan, 2022. Zero-Trust Architecture Application Policy.

[50] Ministry of Education, Culture, Sports, Science and Technology, 2022. MEXT's Mid- to Long-term Plan based on the Priority Plan for Realizing a Digital Society.

[51] Cyber Security Agency of Singapore, 2021. The Singapore Cybersecurity Strategy 2021.

[52] Cyber Security Agency of Singapore, 2022. Cybersecurity Code of Practice for Critical Information Infrastructure - Second Edition Revision One.

[53] Statista, 2023. Statistics report about Zero Trust.

[54] Fortinet, 2023. The State of Zero Trust.

[55] Pokhrel, S. R., Ding, J., Park, J., Park, O. -S. and Choi, J., 2020. Towards Enabling Critical mMTC: A Review of URLLC Within mMTC. in IEEE Access, vol. 8, pp. 131796-131813.

[56] Siddiqi, M. A., Yu, H., & Joung, J., 2019. 5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices. Electronics, vol. 8, no. 9, 981.

[57] Rico, D. and Merino, P., 2020. A Survey of End-to-End Solutions for Reliable Low-Latency Communications in 5G Networks. in IEEE Access, vol. 8, pp. 192808-192834.

[58] Feng, D. et al., Toward Ultrareliable Low-Latency Communications: Typical Scenarios, Possible Solutions, and Open Issues. in IEEE Vehicular Technology Magazine, vol. 14, no. 2, pp. 94-102.

[59] ITU-T, 2021. Requirements and framework for latency guarantee in large-scale networks including the IMT-2020 network. Recommendation ITU-T Y.3113.

[60] Prathyusha, Y. and Sheu, T. -L., 2022. Coordinated Resource Allocations for eMBB and URLLC in 5G Communication Networks. in IEEE Transactions on Vehicular Technology, vol. 71, no. 8, pp. 8717-8728.

[61] Park, J., Samarakoon, S., Shiri, H., Abdel-Aziz, M. K., Nishio, T., Elgabli, A., & Bennis, M., 2022. Extreme ultra-reliable and low-latency communication. Nature Electronics, vol. 5, no. 3, pp. 133-141.

[62] Jun, S., Kang, Y., Kim, J., & Kim, C., 2020. Ultra-low-latency

services in 5G systems: A perspective from 3GPP standards. ETRI journal, vol. 42, no. 5, pp. 721-733.

[63] Kolovou, G., Oteafy, S., & Chatzimisios, P., 2021. A remote surgery use case for the IEEE p1918. 1 tactile Internet standard. In ICC 2021-IEEE International Conference on Communications, pp. 1-6. IEEE.

[64] 3rd Generation Partnership Project (3GPP), 2023. Service requirements for the 5G system. Techinacl Specification, 3GPP TS 22.261, Realse 19(v19.4.0).

[65] Tyler, D., & Viana, T., 2021. Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences, vol. 11, no. 16, 7499.

[66] Chen, B. et al., 2021. A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture. in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10248-10263, 1 July1, 2021.

[67] Yang, D., Zhao, Y., Wu, K., Guo, X. and Peng, H., 2021. An efficient authentication scheme based on Zero Trust for UAV swarm. 2021 International Conference on Networking and Network Applications (NaNA), Lijiang City, China, pp. 356-360.

[68] Li, S., Iqbal, M., & Saxena, N., 2022. Future industry internet of things with zero-trust security. Information Systems Frontiers, pp. 1-14.

[69] Wei, Y. C. and Yu, T. W., 2023. Zero Trust Framework In Financial Sector: The Handling Of Machine Learning Based Trust Management.

2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), PingTung, Taiwan, pp. 211-212.

[70] Buck, C., Olenberger, C., Schweizer, A., V?lter, F., Eymann, T., 2021. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, vol. 110.

[71] Ramezanpour, K., Jagannath, J., & Jagannath, A., 2023. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and rese0arch directions from a coexistence perspective. Computer Networks, vol. 221.

[72] Microsoft, 2023. Data classification & sensitivity label taxonomy [Online]. Available: https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-classification-and-labels

[73] Microsoft, 2023. Data privacy for cloud-scale analytics in Azure [Online]. Available: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/cloud-scale-analytics/secure-data-privacy

[74] Aburukba, R. O., AliKarrar, M., Landolsi, T., & El-Fakih, K., 2020. Scheduling Internet of Things requests to minimize latency in hybrid Fog – Cloud computing. Future Generation Computer Systems, vol. 111, pp. 539-551.

[75] Zhang, W., Liu, Y., Han, G., Feng, Y., & Zhao, Y., 2018. An Energy Efficient and QoS Aware Routing Algorithm Based on Data Classification for Industrial Wireless Sensor Networks. in IEEE

Access, vol. 6, pp. 46495-46504, doi: 10.1109/ACCESS.2018.2866165.

[76] NIST, 2020. Zero Trust Cybersecurity: 'Never Trust, Always Verify [Online]. Available: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

[77] Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M., 2021. Survivable zero trust for cloud computing environments. Computers & Security, vol. 110, 102419.

[78] Jo, G., Shin, J. and Oh, S. -M., 2023. 5G URLLC evolving towards 6G: research directions and vision. 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, pp. 853-855.

[79] Hao, P., Han, X., Xia, S., Ren, M., & Deng, Y., 2020. Performance Evaluation of 5G Ultra-Reliable and Low Latency Communications. In 2020 International Wireless Communications and Mobile Computing (IWCMC), pp. 1047-1052. IEEE.

[80] Feng, D., Lai, L., Luo, J., Zhong, Y., Zheng, C., & Ying, K., 2021. Ultra-reliable and low-latency communications: applications, opportunities and challenges. Science China Information Sciences, vol. 64, pp. 1-12.

ABSTRACT

Dynamic Zero-Trust Cloud Architecture and Access Control Mechanism for Low-Latency and High Reliable Network Services

So-Hui Kim
Department of Future Convergence Technology Engineering
Graduate School of
Sungshin Women's University

As cloud computing devices are connected to ultra-high-speed networks and network perimeters disappear, a new paradigm in cloud security has emerged with the Zero Trust-based access control approach to securely protect digital assets, overcoming the limitations of traditional perimeter-based access control methods. Zero Trust operates on the principle of trusting no one, enforcing a rigorous trust evaluation process for users each time they access cloud resources, providing a high level of security. However, due to the ongoing evaluation and monitoring procedures, there is a trade-off issue that can increase service processing latency. In order to seamlessly support latency-sensitive services in ultra-low-latency network environments, it is necessary to

optimize the trade-off relationship between security and performance. In this paper, we propose the Dynamic Zero Trust Architecture (DZTA), which dynamically applies three different cloud access control policies based on user trust evaluation procedures, considering privacy sensitivity and latency sensitivity, to simultaneously ensure security and performance. To evaluate the effectiveness of cloud access control policies and compare the end-to-end latency and impact of attack between traditional approaches and DZTA, we mathematically modeled the effects and analyzed the performance based on numerical analysis results. As a result, DZTA achieved an average 85% reduction in latency compared to traditional Zero Trust Architecture (ZTA), and the impact of attack decreased by an average of 8200% compared to perimeter-based access control methods.