멀티 클라우드 환경에서의 전송 보안을 위한 PQ-Hybrid TLS 기반 아키텍처 설계

손우영[1], 권순홍[1], 황미녕[2], 이종혁[1]
[1]정보보호학과 & 지능형드론 융합전공, 세종대학교
[2]데이터 플랫폼 센터, 한국과학기술정보연구원
wooyoung@pel.sejong.ac.kr, soonhong@pel.sejong.ac.kr,
mnhwang@kisti.re.kr, jonghyouk@sejong.ac.kr

PQ-Hybrid TLS Based Architecture Design for Transport Security in Multi-Cloud Environments

Wooyoung Son[1], Soonhong Kwon[1], Mi-Nyeong Hwang[2], Jong-Hyouk Lee[1]
[1]Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University
[2]Data Platform Center, Korea Institute of Science and Technology Information

요 약

다양한 클라우드 서비스를 제공하는 멀티 클라우드는 그 특성으로 인해 확장성과 유연성을 제공하고 있다. 하지만, 최근 클라우드 간 데이터 통신 과정에서의 외부 통신 경로가 기하급수적으로 증가하고 있으며, 이는 공격자가 침투할 수 있는 공격 표면을 증가시킴을 의미한다. 이에 현재 TLS (Transport Layer Security) 방식을 통해 데이터 전송 간 보안을 수립하고 있으나, 양자 컴퓨팅 시대가 도래할 경우, 보안성의 붕괴가 발생할 수 있을 것으로 시사된다. 이에 따라 본 논문에서는 양자 컴퓨터 상용화 시대에 대비하여 멀티 클라우드 환경의 전송 보안을 보장할 수 있는 PQ (Post-Quantum)-Hybrid TLS 기반 아키텍처를 설계한다. 보다 세부적으로 제안된 아키텍처는 멀티 클라우드 보안을 3가지 Trust Boundary로 구분하고 각 경계에서 발생 가능한 보안 위협 및 이를 보완하기 위한 통신 보안 기법을 제안하였다. 또한, 기존 TLS와 제안하는 PQ-Hybrid TLS 간의 핸드쉐이크 성능을 비교/분석함으로써 PQ Cryptography 기반 통신의 전환은 합리적이고 필수적임을 제시한다.

1. 서론

멀티 클라우드는 2개 이상의 클라우드 서비스를 동시에 활용할 수 있게 하는 개념으로 서비스의 확장성과 유연성을 제공한다. 하지만, 이는 반대로 멀티 클라우드 환경은 공격자의 타겟이 될 수 있는 공격 표면이 넓다는 한계점으로 직결될 수 있다. 보다 세부적으로 다수 클라우드 간의 API (Application Programming Interface) 연동 및 외부 데이터베이스와의 연계 등은 외부 통신 경로를 기하급수적으로 증가시키며, 이는 공격자가 침투 가능한 지점을 크게 넓히고 있다. 이를 보완하기 위해 기존 API를 기반으로 하던 통신을 넘어 TLS (Transport Layer Security)를 통해 통신의 보안성을 높이고자 하였으나, 해당 보안 통신 기법 또한 양자 컴퓨팅 시대가 도래할 시 보안성의 붕괴로 이어질 가능성이 존재한다. 비용 절감 및 높은 접근성을 지닌다는 클라우드의 특성으로 인해 최근에는 많은 기업을 넘어 국가 공공기관에서도 클라우드 기술을 사용하고 있다. 이에 따라 국가 핵심 정보까지 클라우드에 저장되는 상황에서, 양자 컴퓨팅으로 인한 기존 통신 보안체계의 붕괴는 치명적인 기밀성 상실을 의미한다.

이에 따라 본 논문에서는 양자 컴퓨팅 시대에도 멀티 클라우드 환경의 전송 보안을 보장하기 위해 PQ (Post-Quantum)-Hybrid TLS 기반 아키텍처를 설계한다. 이를 위해 멀티 클라우드 보안을 세 가지 Trust Boundary로 구분하고, 각 경계에서 발생 가능한 보안 위협과 이에 대응하기 위한 통신 보안 기법을 제안한다. 또한, 기존 TLS와 제안하는 PQ-Hybrid TLS의 핸드쉐이크 성능을 비교/분석하여 PQ-Hybrid TLS가 다소 성능 저하를 수반하더라도 그 영향은 실제 환경에서 미미함을 보인다. 더 나아가, 이러한 단기적 성능 저하보다 장기적인 기밀성 상실 위험이 훨씬 큰 비용을 초래함을 논증함으로써 멀티 클라우드 보안에서의 PQC (Post-Quantum Cryptography) 기반 통신으로의 전환은 합리적이고 필수적임을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 멀티 클라우드 통신 보안 기능을 구성하는 기술에 대해 분석하며, 3장에서는 본 논문에서 제안하는 아키텍처에 대하여 주요 프레임워크와 함께 설명한다. 4장에서는 기존 TLS 방식과 제안된 PQ-Hybrid TLS에 대하여 핸드쉐이크 성능 비교를 수행한 결과에 대해 논의하며, 5장에서는 본 논문의 결론을 맺는다.

2. 멀티 클라우드 통신 보안 분석

멀티 클라우드 환경에서의 보안 통신은 오늘날 API 중심 연동이 주류를 이룬다. AWS, Azure, GCP와 같은 주요 Cloud Service Provider들은 각자의 API 게이트웨이와 관리 서비스를 제공하며, 기업들은 이를 통해 이기종 클라우드 간 데이터와 워크로드를 연결한다. 이렇듯 API는 멀티 클라우드 연동의 중심축이지만, 동시에 클라우드 서비스 간 일관되지 않은 보안 정책이라는 구조적 제약을 가진다. 인증 시 AWS Cognito, 접근 제어 시 Azure API Management를 혼용할 경우, 상호 간 사용자 권한 동기화가 원활히 이루어지지 않아 정책 불일치 및 설정 오류가 발생할 수 있다. 이러한 불일치는 곧 일관된 인증/인가/모니터링 부재로 이어지며, 멀티 클라우드 환경에서의 API 보안을 취약하게 만든다 [1].

이와 같은 상황에서의 핵심 문제는 이러한 복잡성이 단순히 운영 부담에 그치지 않는다는 점이다. 멀티 클라우드 환경은 다양한 클라우드 서비스를 사용한다는 특성상 API 노출을 필연적으로 확대시키며, 이는 곧 공격 표면의 확장을 의미한다. OWASP API Security Top 10은 객체 수준 권한 부여(API1:2019)와 사용자 인증 취약점(API2:2019)을 치명적인 보안 위험 요소로 지적한 바 있다 [2]. 실제로 페이스북에서 발생한 API 취약점 사례는 이를 단적으로 보여준다 [1]. 당시 공격자는 손상된 인증 토큰을 악용하여 수백만 명의 개인정보에 무단 접근할 수 있었으며, 이는 단일 플랫폼에서도 대규모 피해를 일으켰다. 멀티 클라우드와 같이 API가 다층적으로 얽히고 노출이 증가하는 환경에서는, 이와 유사한 공격이 훨씬 더 빈번하게 재현될 수 있다는 점에서 그 위협은 한층 심각하다. 결국 API 중심의 멀티 클라우드 구조는 본질적으로 데이터 탈취와 무단 접근에 취약한 속성을 내재하고 있다고 볼 수 있다.

따라서, 최근 멀티 클라우드 관련 보고서 및 보안 가이드에서는 API 통신을 넘어 TLS 기반 암호화의 필요성을 강조한다. CogentInfo는 클라우드 간 API 트래픽이 노출될 경우 데이터 탈취 위험이 치명적이므로, 모든 멀티 클라우드 API 연동은 TLS 1.2 또는 TLS 1.3을 통해 보호해야 한다고 권고하고 있다 [1]. 또한, Cisco의 Multicloud Defense 백서 역시 멀티 클라우드 게이트웨이를 경유하는 데이터 흐름을 전제로, TLS의 필요성을 강조하며 역방향·순방향 프록시 구조에 TLS와 PFS (Perfect Forward Secrecy)를 결합하여 트래픽을 심층적으로 검사하고 보호하는 방안을 제시한다 [3]. 더 나아가, AWS와 GCP 간 통신에 mTLS (Mutual TLS)를 적용하여 클라우드 간 API 호출에서 데이터 암호화 뿐만 아니라 양방향 인증까지 보장하려는 시도가 이루어지고 있다 [4]. 이처럼 최근에는 멀티 클라우드 간 데이터 교환 구간에서 TLS, 나아가 mTLS를 사실상의 표준 보안 메커니즘으로 간주하며, 이는 다양한 이기종 환경을 연결하는 최소한의 보안선 역할을 하고 있다.

[표 1] TLS 1.2/1.3, mTLS 및 PQ-TLS의 보안 기능 비교

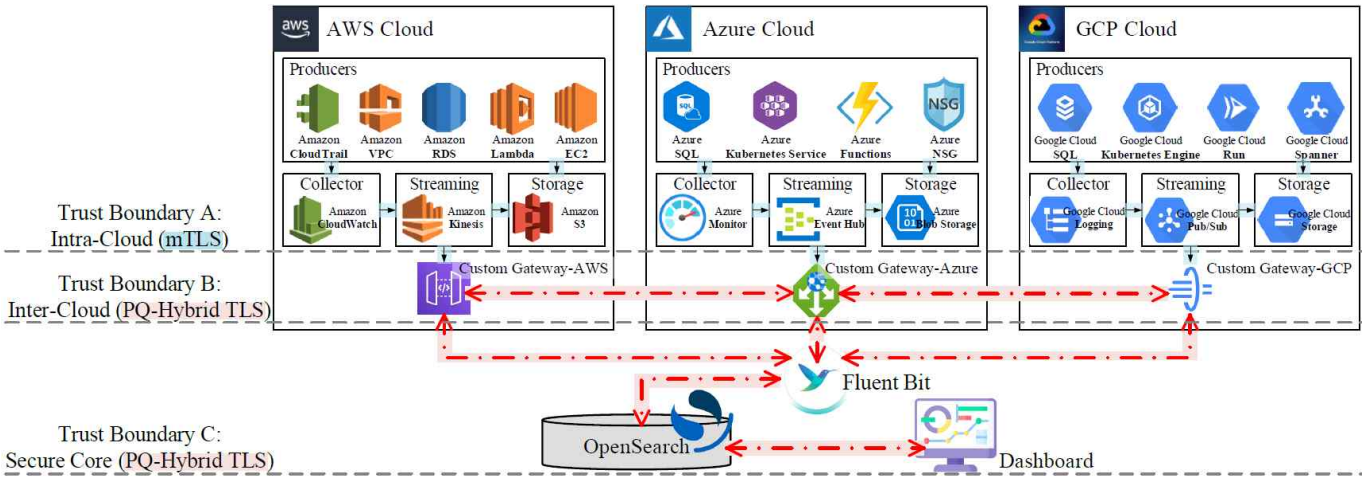
구분	TLS 1.2/1.3	mTLS	PQ-TLS
데이터 암호화	지원	지원	지원
서버 인증	지원	지원	지원
클라이언트 인증	제한적	강제됨	강제됨
PFS	지원	지원	지원
양자 내성	없음	없음	있음 (PQC 기반)

그러나 이 모든 노력에도 불구하고, 클라우드 간 전송 구간의 암호 강도는 여전히 전통적인 TLS에 기반한다는 한계점이 존재한다. [표 1]은 멀티 클라우드에서 일반적으로 사용되는 전송 보안 메커니즘인 TLS 1.2/1.3, mTLS 및 본 논문에서 제안하는 PQ-TLS의 주요 보안 기능을 비교한 것이다. [표 1]에서 확인할 수 있듯이, 기존 TLS 계열과 mTLS는 데이터 암호화, 서버 인증, PFS 등을 제안하지만, 이들 프로토콜은 양자컴퓨팅의 발전 앞에서는 근본적으로 취약하다. 다시 말해, 멀티 클라우드 환경은 API 거버넌스와 TLS 기반 암호화라는 이중 보호 장치를 갖추고 있음에도 불구하고, 양자 이후(Post-Quantum) 시대를 전제로 한 전송 보안을 제공하지 못한다는 한계점이 존재한다. 이는 곧 미래 멀티 클라우드 보안의 지속 가능성을 위협하는 치명적 공백으로, 멀티 클라우드 환경에서의 PQC 기반 TLS, 즉 PQ-TLS 아키텍처의 필요성을 강조한다.

3. 제안하는 아키텍처

현재 대부분의 멀티 클라우드 환경에서의 통신 보안은 TLS에 의존하고 있으나, 이는 양자 컴퓨팅이 본격적으로 사용될 경우, 보안성을 유지할 수 없다는 한계점을 지닌다. 이러한 문제의식을 바탕으로 본 논문에서는 PQ-Hybird TLS를 적용한 멀티 클라우드 보안 아키텍처를 제안한다. 이를 통해 양자 이후 시대에서도 데이터 통신의 보안성을 유지할 뿐만 아니라, 선 수집 후 해독 공격인 Harvest Now, Decrypt Later 공격에도 대응 가능할 것으로 판단된다. (그림 1)은 PQ-Hybrid TLS 기반 멀티 클라우드 아키텍처의 전반적인 구조를 나타낸다.

제안하는 아키텍처에서의 멀티 클라우드 환경은 AWS, Azure, GCP의 세 가지 클라우드 서비스로 구성된다. 각 클라우드는 서로 다른 네트워크 구조, API 인증 체계, 인증 방식을 지니므로, 독립적인 게이트웨이를 두어 관리하도록 설계하였다. 이러한 분리 구조는 먼저, PQ-Hybrid TLS 적용 시 트래픽이 각 게이트웨이로 분산되어 세션 핸드쉐이크 과정 시, 처리 효율성이 향상된다는 이점을 지닌다. 또한, 특정 클라우드에서 보안 사고가 발생하는 경우, 해당 게이트웨이만을 폐쇄하여 대응 가능함에 따라 전체 멀티 클라우드 서비스의 가용성과 서비스 연속성을 유지할 수 있다. 이렇게 분리된 3개 클라우드 서비스의 게이트웨이에서 수집된 로그 데이터는 경량 고성능 로그 수집 및 전처리 도구인 Fluent



(그림 1) 제안하는 멀티 클라우드 환경에서의 PQ-Hybrid TLS 기반 아키텍처

Bit를 통해 통합 로그 분석을 위한 OpenSearch에 전송된다. 이를 통해 다양한 클라우드 환경에서 수집되는 분산된 로그 데이터를 하나의 분석 지점에서 집약하여 저장 및 분석함으로써 공격의 전체적인 흐름을 명확히 파악하고, 고도화된 위협 분석 및 예측을 가능하도록 한다.

제안하는 아키텍처는 먼저 멀티 클라우드 보안에 대해 세가지 Trust Boundary로 구분하고, 구분된 경계 구간의 특성에 따라 발생 가능한 보안 위협 및 이를 보완하기 위한 통신 보안 기법에 대한 설계를 진행하였다. 첫 번째 경계 구간인 Trust Boundary A: Intra-Cloud에서는 단일 클라우드 내부에서의 로그 생성, 수집, 스트리밍 및 저장소 간 데이터 이동이 이루어진다. 이에 따라 해당 구간에서는 내부자 공격에 의한 데이터 위변조, 다계층 서비스 간 신뢰 붕괴가 주요 위협으로 작용된다. 이에 따라 Boundary A에는 현존하는 보안 통신 기법 중 고도화된 기법인 mTLS를 적용하였다. mTLS는 인증서 기반 양방향 검증을 통해 통신 무결성과 접근 제어를 동시에 보장하며, 내부 공격 및 자격 증명 탈취 위험을 최소화한다.

두 번째 구간인 Trust Boundary B: Inter-Cloud의 경우, AWS, Azure, GCP 간 데이터 교환이 발생하는 영역이다. 이에 따라 해당 영역은 외부 노출 빈도가 높고, 이는 Trust Boundary A에 비하여 더 넓은 공격 표면을 지님을 의미한다. 특히, 각 클라우드의 게이트웨이를 통해 상호 연동되는 이 구간에서는 네트워크 수준 도청, 중간자 공격 및 인증서 위/변조 시도와 같은 보안위협이 발생할 수 있다. 이에 따라 기존 TLS 만으로는 양자 컴퓨터 등장 시 보안성이 붕괴될 수 있으므로, 본 연구에서는 Boundary B에 PQ-Hybrid TLS를 적용하였다. 이를 통해 클라우드 간 데이터 교환이 양자 안전성을 확보한 암호 채널 위에서 수행되며, 외부 공격자에 의한 통신 도청 및 위변조, 향후 양자 컴퓨팅 위협에까지 현재와 미래의 위협 모두에 포괄적으로 대응할 수 있을 것으로 판단된다.

마지막으로, Trust Boundary C: Secure Core는 멀티 클라우드 데이터가 집약적인 저장 및 분석을 위해 하나의 분석 지점인 OpenSearch와 시각화를 위한 대시보드로 전달되는 영역이다. 해당 구간은 보안 분석 코어와 외부 도구가 직접 연결되는 만큼 공격자가 가장 쉽게 접근 가능한 진입점이 된다. 특히 대시보드를 통한 민감 데이터 접근 및 분석 결과 위조와 같은 치명적인 보안 위협이 발생할 것으로 판단됨에 따라 Boundary C 역시 PQ-Hybrid TLS를 적용하여, 클라우드에서 보안 코어로 이동하는 모든 데이터가 양자 안전성을 유지한 상태로 전송되도록 보장하고자 하였다.

결국, 제안하는 아키텍처는 Boundary A에서 현존 위협에 대응하는 mTLS, Boundary B와 C에서 양자 시대 위협까지 대비하는 PQ-Hybrid TLS라는 이중 전략을 채택한다. 이를 통해 내부자 공격부터 외부의 양자 기반 공격에 이르기까지 전 구간을 포괄하는 다층적 보안 프레임워크를 제공하며, 결과적으로 멀티 클라우드 환경의 지속 가능하고 미래지향적인 보안성을 보장할 수 있을 것으로 판단된다.

4. 실험 결과 및 분석

멀티 클라우드 환경에서 안전한 데이터 전송을 보장하기 위해 본 논문에서는 PQ-Hybrid TLS를 적용하였다. 이는 양자 컴퓨터가 상용화될 것을 예상하여 TLS가 무력화될 가능성이 존재함에 따라 이에 대한 대비는 필수적이라고 할 수 있다. 이에 클라우드 간 데이터 연동이나 핵심 전송 경로에 대해 PQ KEM인 Kyber 768을 기존 ECDHE X25519와 결합한 하이브리드 키 교환 방식(ECDHE X25519+Kyber768)을 적용함으로써, 데이터 전송 구간의 안전성을 확보하고자 하였다.

(그림 1)를 통해 확인할 수 있듯이, 각 클라우드 상에서 발생하는 이벤트, 보안 위협 로그 등의 민감 데이터들은 클

```
Algo,Rounds,TotalTime(s),AvgHandshake(ms)
X25519,100,1,10.000

Algo,Rounds,TotalTime(s),AvgHandshake(ms)
x25519_kyber768,100,2,20.000
```

(그림 2) Classic TLS와 PQ-Hybrid TLS 방식의 핸드쉐이크 성능 비교 결과

라우드 별 게이트웨이를 거쳐 전송된다. 이에 본 논문에서는 각 게이트웨이에 대하여 컨테이너화하여 구성하였으며, 이에 대한 당위성을 제시하기 위해 Classic TLS (ECDHE X25519)와 제안된 PQ-Hybrid TLS (ECDHE X25519+Kyer768) 방식을 비교하였다. 이를 위해 클라이언트가 연결을 시도한 시점부터 핸드쉐이크가 완료되어 세션 키가 확정되기까지의 전체 시간의 평균을 의미하는 핸드쉐이크 시 발생하는 총 평균 소요시간과, 핸드쉐이크 메시지 단위의 네트워크 왕복 지연 및 서버 처리 지연의 평균을 의미하는 평균 핸드쉐이크 지연 시간을 측정하였으며, 평균 값을 도출하기 위해 총 100회의 실험을 진행하였다.

(그림 2)는 순서대로 Classic TLS (ECDHE X25519)와 제안된 PQ-Hybrid TLS (ECDHE X25519+Kyer768)의 핸드쉐이크 성능을 도출한 결과로, 총 평균 소요시간과 평균 핸드쉐이크 지연 시간의 차이를 보여준다. 실험 결과, ECDHE X25519 기반 TLS는 총 평균 소요시간이 1초, 평균 핸드쉐이크 지연 시간이 10ms로 측정되었다. 반면, X25519_Kyber768 기반 PQ-Hybrid TLS는 총 평균 소요시간이 2초, 평균 핸드쉐이크 지연시간은 20ms로 측정되었다. 이는 PQ-Hybrid TLS가 기존 방식 대비 성능 저하를 수반함을 보여준다. 그러나 실제 멀티 클라우드 네트워크에서는 수십~수백 ms 수준의 지연이 기본적으로 존재하기 때문에, 앞서 도출된 추가 비용은 전체 운영 성능에 미치는 영향이 제한적이라고 평가할 수 있다.

따라서, 본 실험 결과로부터 두 가지 중요한 시사점을 도출할 수 있다. 첫째, 양자 컴퓨터 상용화 시대를 대비하여 TLS 보안을 강화하는 것은 성능 저하보다 훨씬 중요한 우선 과제라는 점이다. 실증을 기반으로 PQ-Hybrid TLS 적용 시 기존 TLS에 비하여 지연이 두 배 증가한 것을 확인하였으나, 실제 네트워크 지연 범위 내에서는 체감 차이가 크지 않을 것임을 앞서 언급한 바 있다. 반면, 기존 RSA/ECDSA 기반의 키교환/서명 알고리즘은 양자 알고리즘에 의해 근본적으로 붕괴될 수 있으며, 이는 현재 전송되는 민감 정보가 장기적으로 유출되어 복호화하는 위험으로 이어질 수 있다. 즉, 단기적인 응답성 저하(수십~수백 ms 증가)와 비교할 때, 데이터가 영구적으로 무력화되는 위험인 장기적인 기밀성 상실은 훨씬 큰 비용이므로, PQC 기반 통신의 전환은 합리적이고 필수적인 선택이다.

둘째, 운영적 관점에서 PQ-Hybrid TLS는 실험 결과에서 확인한 바와 같이 기존 TLS 방식 대비 추가 지연을 수반한다. 이러한 지연은 서비스 편리성이 강조된 클라우드 환경에서 사용자 경험 저하로 직결될 수 있다는 점에서 한계로 작용한다. 따라서, PQ-Hybrid TLS는 모든 구간에 일괄적으로 적용하기 보다, 외부 노출 빈도가 높고 민감 데이터가 교차하는 Inter-Cloud 및 Secure Core 구간에 우선 적용하고, Intra-Cloud 내부 구간에는 mTLS를 유지하는 선별적 적용 전략 방식이 바람직하다. 이를 통해 비용, 성능 및 보안의 균형을 달성할 수 있을 것으로 판단된다.

5. 결론

본 논문은 멀티 클라우드 환경에서 양자 컴퓨팅 시대를 대비한 전송 보안 방안을 제시하기 위해 PQ-TLS 기반 아키텍처를 설계하였다. 이를 위해 멀티 클라우드 보안을 세 가지 Trust Boundary로 구분하고, 각 경계에 대한 통신 보안 기법을 체계적으로 제안하였으며, 실증을 기반으로 제안된 PQ-Hybird TLS와 기존 TLS와의 핸드쉐이크 성능을 비교/분석하였다. 이에 따라 본 연구는 멀티 클라우드 환경에서의 지속 가능한 전송 보안 확보를 위해 멀티 클라우드 환경을 체계적으로 정의하고 PQC 기반 보안 프로토콜 도입의 필요성을 실증적으로 뒷받침하였다는 점에서 의의를 지닌다. 향후 연구에서는 다양한 PQC 알고리즘과 하이브리드 구성 방식을 적용하여 멀티 클라우드 아키텍처 전반에서의 성능/보안 균형을 최적화하는 방안에 대한 연구를 수행할 예정이다.

Acknowledgement

본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2025년도 문화기술 연구개발사업으로 수행되었음 (과제명: On-Device AI 모델 저작권 보호 및 관리를 위한 글로벌 인재양성, 과제번호: RS-2025-02221620, 기여율: 50%). 이 연구는 한국과학기술정보연구원의 지원을 받았습니다 (과제번호: (KISTI)J25JR001-25, 기여율: 50%).

참고문헌

[1] “Securing APIs in Complex, Multi-Cloud Environments”, [Online]. Available: https://www.cogentinfo.com/resources/securing-apis-in-complex-multi-cloud-environments [Accessed: Sep. 16, 2025].
[2] “OWASP Top 10 API Security Risks – 2019”, [Online]. Available: https://owasp.org/API-Security/editions/2019/en/0x11-t10/ [Accessed: Sep. 16, 2025].
[3] “Cisco Multicloud Defense White Paper”, [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/multicloud-defense/multicloud-defense-wp.html [Accessed: Sep. 17, 2025].
[4] “mTLS for Multi-Cloud Security”, [Online]. Available: https://akashchaurasia9336.medium.com/mtls-for-multi-cloud-security-secure-communication-between-aws-and-gcp-6d0c39fa1f3a [Accessed: Sep. 17, 2025].