MITRE ATT&CK 기반 주요 클라우드 벤더별 공격 표면 및 공격 벡터 비교 분석

지동혁*, 최상훈[1], 박기웅†

세종대학교 SysCore Lab. (대학원생, 연구 교수[1])

**세종대학교 정보보호학과 (교수†)

MITRE ATT&CK-Based Comparative Analysis of Attack Surfaces and Attack Vectors Across Major cloud Providers

Dong-Hyeok Ji*, Sang-Hoon Choi[1], Ki-Woong Park†

* Syscore Lab., Sejong University
**Dept. of Computer and Information Security, Sejong University
(Graduate Student*, Research Professor[1], Professor†)

요 약

최근 기업들이 클라우드 서비스를 도입하면서, 단일 클라우드 환경보다는 다중 클라우드 서비스를 활용해 부서별 요구사항을 충족시켜 주는 멀티 클라우드 환경 도입이 증가하고 있다. 하지만 기존 연구는 단일 환경에 해당하는 연구가 대부분이다. 따라서, 본 연구는 AWS, GCP, Azure의 아키텍처를 대상으로 공격 표면과 공격 벡터를 비교, 분석하였다. 각 플랫폼의 Well-Architected Framework를 세 영역으로 분류하고, 공격 벡터를 MITRE ATT&CK ID와 매핑하였다. 분석 결과, 세 플랫폼 공통으로 발견된 공격 벡터가 있었으며, 특정 플랫폼에서만 나타나는 공격 벡터도 확인되었다. 이를 바탕으로 플랫폼 선택 기준을 제시하고 향후 연구 방향을 논의한다.

I. 서론

최근 기업의 IT 인프라 환경은 온프레미스에서 클라우드 환경으로 전환되고 있다. 똑같이 기업에서도 부서별 요구사항이 다양해지면서 여러 클라우드 서비스를 사용하는 멀티 클라우드 환경도 증가하고 있다 [1]. 한편, AWS, GCP, Azure와 같은 주요 클라우드 서비스 사업자는 서로 다른 아키텍처와 보안 정책을 기반으로 서비스를 운영한다. 이에 따라 기업은 이러한 차이를 고려한 인프라를 마련해야 한다 [2]. 또한, 동일한 목적의 아키텍처라도, 제공되는 구성 요소에 따라 노출되는 공격 표면(Attack Surface)이 달라진다 [3, 4]. 공격자는 벤더사 구조의 차이를 분석하고, 이에 맞는 공격 벡터(Attack Vector)를 선택해 침투를 시도한다. 따라서 보안 위협이 다르게 나타나는 만큼, 인프라 선택에 관한 연구가 필요하다. 그러나 기존 연구는 대부분 단일 클라우드 환경에서의 공격 표면이나 공격 벡터에 집중되어 있고, 여러 환경을 분석한 연구는 드문 편이다. 이로 인해 실제 환경에서 플랫폼을 선택하거나 인프라를 설계할 때 참고하기에는 한계가 있다. 본 연구는 이러한 한계를 보완하고자, AWS, GCP, Azure의 공식적인 문서에 근거해 두 가지 아키텍처를 비교 대상으로 선정하였다.

우리는 각 플랫폼의 Well-Architected Framework를 바탕으로 IaaS 기반 3-Tier 웹 애플리케이션과 서버리스(Serverless) 기반 웹/API 구조 아키텍처를 선정했다. 그리고 공격 표면을 세 가지 Edge, Identity & Management(이하 I & M), Data로 통일하여 분류하였다. 분류 기준은 다음과 같다. Edge 영역은 인터넷 또는 외

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 논문은 과학기술정보통신부의 재원으로 실감콘텐츠핵심기술개발 (Project No. RS-2023-00228996, 40%), 국방ICT융합연구(Project No. 2022-11220701, 30%), 한국콘텐츠진흥원(KOCCA) 저작권기술 글로벌 인재 양성사업 (Project No. RS-2025-02221620, 30%)의 지원을 받아 수행된 연구임.

부 네트워크에서 직접 접근 가능한 퍼블릭 엔드포인트처럼 외부 트래픽이 최초로 유입되는 경계 지점에 해당한다. I & M 영역은 계정, 역할, 정책 등 인증, 인가 및 제어 면에서의 접근 통제를 담당하는 요소이다. Data 영역은 오브젝트 스토리지, DB 등 데이터를 저장 보관하는 계층이다. 이러한 중요 계층을 통해 공격 벡터를 식별하고 비교한 후 플랫폼 선택과 인프라 설계 시 우선순위를 제시한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 설명하고, 3장에서는 아키텍처별 공격 표면과 공격 벡터를 정리하며, 4장에서는 결론과 향후 연구 방향을 제시한다.

II. 관련 연구

2.1 클라우드 환경에서 공격표면 관련 연구

2023년, Everson 등은 인터넷에 노출된 서비스 등을 수집해 식별 → 분류 → 그래프화로 이어지는 외부 공격 표면 절차를 제안하였다 [3]. 정확도 지표와 대규모 스캐닝의 윤리, 법적인 부분까지 포함한 절차를 표준화하였다.

2023년, Morteza 등은 스캔을 활용한 인터넷 측정 기반 보안 연구를 하였다 [4]. 이를 통해 클라우드 환경에서 외부 공격 표면을 데이터 기반으로 추정할 수 있다는 결론을 내렸다.

2.2 클라우드 구성 요소 별 공격 벡터 연구

2024년, Ni 등은 서버리스 환경을 추상 모델로 정의하고, 이벤트 인젝션 등 서버리스의 공격 벡터를 모델링하였다 [5]. 이를 통해 서버리스 기반 웹/API 아키텍처에서 어떤 벡터가 상대적으로 위험한지 우선순위를 제시하였다.

2023년, Minna 등은 마이크로서비스 런타임 보안을 정리하면서, 서비스 간 인증 등 운영 시점의 공격 벡터를 정리하였다 [6].

2.3 클라우드 정책 관점에서의 관련 연구

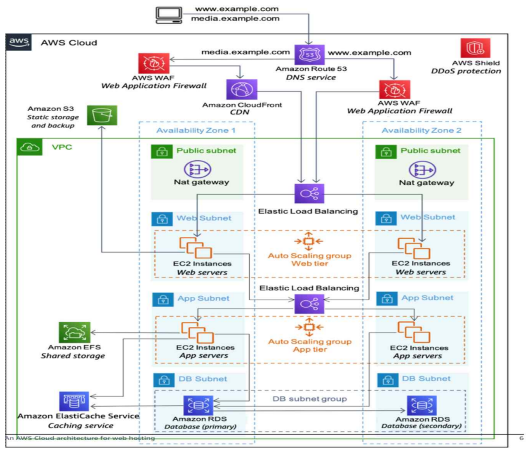
2024, Ali 등은 ISO/IEC 27005 등 리스크 평가 방법을 클라우드 맥락으로 비교하고 식별, 분석, 대응 절차의 틀을 제시하였다 [7]. 이는 동일한 공격 표면, 공격 벡터를 같은 절차로 점수화하여 우선 수위를 매기기 위한 것이다.

2023년, Rahaman 등은 클라우드-네이티브의 접근제어 정책을 체계화하여 공격 표면에서 인증 우회, 시크릿 유출 등 공격 벡터를 정책 설계로 축소하는 방안을 제시했다 [8].

III. 클라우드 벤더별 공격 표면과 공격 벡터

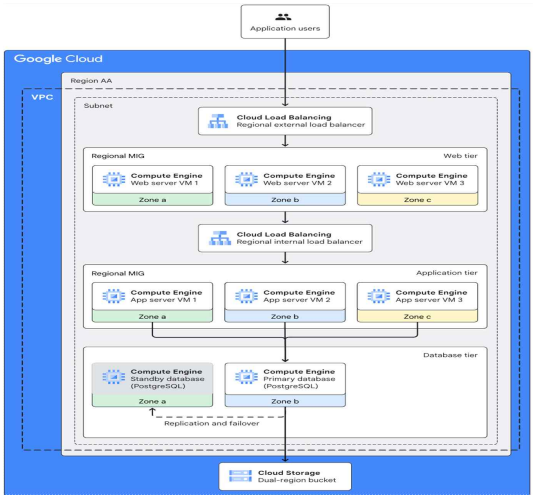
3.1 IaaS 기반 3-Tier 웹 애플리케이션

AWS, Edge의 구성 요소는 Route 53, Cloud Front, 외부 ALB로 (그림 1)과 같다 [9]. 공격 벡터는 퍼블릭 웹 취약점 악용인 T1190, 무차별 공격인 T1110이 있다. I & M의 구성 요소는 IAM 사용자, 그룹, 역할, STS AssumeRole 등이 있다. 공격 벡터는 유효 계정 남용인 T1078, 또한 자격증명 노출인 T1552가 있다. Data의 구성 요소는 S3, RDS 등으로 (그림 1)의 하단부에 있고, 공격 벡터는 클라우드 스토리지 객체 유출인 T1530, 데이터 탈취인 T1213이 있다.



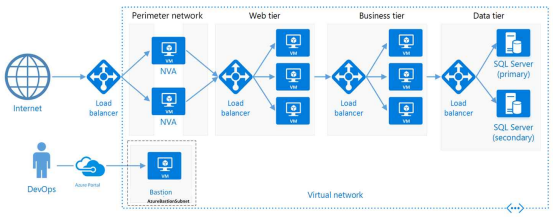
(그림 1) AWS IaaS 기반 웹 아키텍처

GCP, Edge의 구성 요소는 Load Balancer로 (그림 2)와 같고, 공격 벡터는 T1190, T1110이 있다 [10]. I & M의 구성 요소는 IAM, Service Account가 있고, 공격 벡터는 T1078.004, 정책 조작으로 지속성 확보인 T1098, 컴퓨터 인프라 변경인 T1578 등이 있다. Data의 구성 요소는 (그림 2)와 같이 하단부의 Cloud Storage가 있다. 공격 벡터는 클라우드 스토리지 객체 접근, 유출인 T1530, T1213, 스토리지를 유출인 T1567이 있다.



(그림 2) GCP IaaS 기반 웹 아키텍처

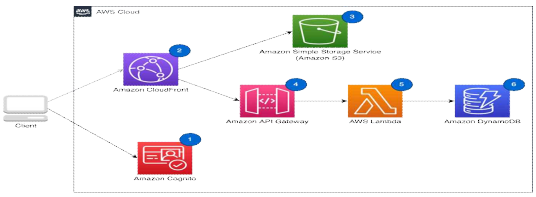
Azure, Edge의 구성 요소는 Load Balancer, 가상방화벽인 NVA로 (그림 3)과 같다 [11]. 공격 벡터는 T1190, T1110이 있다. I & M의 구성 요소는 Entra ID, 리소스 관리 서비스인 ARM, 인스턴스에 대한 정보를 제공하는 IMDS가 있다. 공격 벡터는 T1078.004, T1098, T1578, 메타데이터 토큰 탈취인 T1552.005가 있다. Data의 구성 요소는 SQL Server 등(그림 3)에 있고, 공격 벡터는 T1213, T1567, T1530이 있다.



(그림 3) Azure IaaS 기반 웹 아키텍처

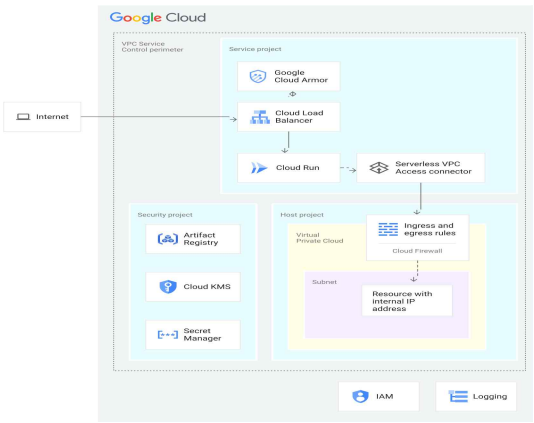
3.2 서버리스 기반 웹/API 구조 아키텍처

AWS, Edge의 구성 요소는 Cloud Front, API Gateway로 (그림 4)와 같다 [9]. 공격 벡터는 T1190, T1550, 크리덴셜 스터핑 공격인 T1110.003이 있다. I & M의 구성 요소는 Cognito, IAM 역할, Lambda 실행 역할, Lambda 권한 이 있다. 공격 벡터는 T1078.004, T1098, T1552, T1578이 있다. Data의 구성 요소는 S3, DynamoDB가 있고, 공격 벡터는 T1530, T1213, T1567이 있다.



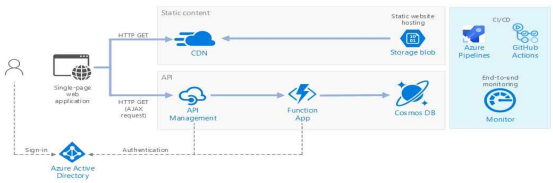
(그림 4) AWS 서버리스 기반 웹 아키텍처

GCP, Edge의 구성 요소는 Load Balancer, Cloud Armor로 (그림 5)와 같다 [10]. 공격 벡터는 T1190, T1110이 있다. I & M의 구성 요소는 IAM, Cloud Run 등이 있다. 공격 벡터는 T1078.004, T1098, 등이 있다. Data의 구성 요소는 Cloud SQL, Storage 등이 있다. 공격 벡터는 T1213, T1530, T1567이 있다.



(그림 5) GCP 서버리스 기반 웹 아키텍처

Azure, Edge의 구성 요소는 CDN, API Management 등으로 (그림 6)과 같고, 공격 벡터는 T1190, T1110이 있다 [11]. I & M의 구성 요소는 Function App 실행권한 등이 있고, 공격 벡터는 T1078, T1098, T1578, T1552가 있다. Data의 구성 요소는 Storage Blob, Cosmos DB가 (그림 6)에 있고 공격 벡터는 T1530, T1213, T1567이 있다.



(그림 6) Azure 서버리스 기반 웹 아키텍처

3.3 클라우드 벤더별 공격 벡터 비교 결과

영역	벡터 ID	벡터 이름
Edge	T1190, T1110	공개 웹 취약점, 무차별 대입
I & M	T1078, T1098	계정 탈취 권한, 정책 조작
Data	T1530, T1213, T1567	스토리지 정보 수집, 유출

(표 1) 벤더에서 나온 공통 벡터

벤더/영역	벡터 ID	벡터 이름
AWS/ Edge	T1550, T110.003	대체 인증 재사용, 크리덴셜 스터핑
GCP	없음	없음
Azure/ Data	T1552.005	IMDS 메타데이터 토큰 노출

(표 2) 특정 벤더에서 나온 벡터

IV.결론 및 향후 연구

본 논문은 각 벤더의 영역을 기준으로 (표 1)의 벤더에서 나온 공통 벡터와 (표 2)의 특정 벤더에서 나온 공격 벡터를 구분해 제시하였다. AWS는 계정, 정책 변경 등 제어 면에서의 거버넌스 리스크가 높았다. GCP는 특정 벡터는 없지만 서버리스 경로에서의 키, 토큰 최소화 필요성이 발견됐고, Azure는 IMDS 기반의 토큰 노출이 발견되었다. 따라서 거버넌스 감사추적이 목적이라면 AWS, 최소 권한과 서버리스 중심의 가벼운 서비스라면 GCP, 중앙집중 ID 거버넌스와 운영 일관성이 중요하면 Azure가 적합하다는 결론을 도출하였다. 향후 연구로는 공격 표면을 세분화하고, 공격 벡터 항목을 확장하여 벤더별 위협 유형의 모호성을 줄일 예정이다. 또한 각 벡터 매핑의 근거를 로그나 공격 사례를 명시해 논리성을 강화 하고자 한다.

[참고문헌]

[1] J.Alonso, Understanding the challenges and novel architectural models of multi-cloud native applications, Journal of Cloud Computing, January, 2023.

[2] S.Deng, H.Zhao, B.Huang, C.Zhang, F.Chen, Y.Deng, J.Yin, S.Dustdar and A.Y.Zomaya, Cloud-native computing: a survey from the perspective of services, Proceedings of the IEEE, January, 2024.

[3] D.Everson and W.Cheng, A survey on network attack surface mapping, Digital Threats: Research and Practice, June, 2024.

[4] M.S.Pour, C.Nader, K.Friday, Internet measurement techniques for cyber security: a survey, Computers & Security, May, 2023.

[5] K.Ni, S.Mondal, H.M.D.Kabir, T.Tan and H.-N.Dai, Toward security quantification of serverless computing, Journal of Cloud Computing, September, 2024.

[6] F.Minna, F.Massacci, SoK: run-time security for cloud microservices. Are we there yet?, Computers & Security, 2023

[7] T.Ali, M.Al-Khalidi and R.Al-Zaidi, Information security risk assessment methods in cloud computing: comprehensive review, Journal of Computer Information Systems, March, 2024.

[8] M.S.Rahaman, S.N.Tisha, E.Song and T.Cerny, Access Control Design Practice and Solutions in Cloud-Native Architecture: A Systematic Mapping Study, Sensors, March, 2023.

[9] Amazon Web Services, AWS Well-Architected Framework, AWS Documentation, November, 2024.

[10] Google Cloud, Google Cloud Well-Architected Framework, Google Cloud Documentation, October, 2024.

[11] Microsoft, Azure Well-Architected Framework, Microsoft Learn, November, 2024.