Journal of Convergence for Information Technology
Vol. 11. No. 7, pp. 7-13, 2021
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.07.007

클라우드 서비스 보안을 위한 AWS 보안 아키텍처 구성방안

박세준[1], 이용준[2*], 박연출[3]
[1]SK 정보보호담당 박사, [2]극동대학교 해킹보안학과 교수, [3]LG 로봇선행연구소 박사

Configuration Method of AWS Security Architecture for Cloud Service

Se-Joon Park[1], Yong-Joon Lee[2*], Yeon-Chool Park[3]
[1]Ph.D, Information Security Group, SK
[2]Professor, Department of Hacking Security, Far East University
[3]Ph.D, Advanced Robotics LAB, LG

요 약 최근 클라우드 컴퓨팅의 다양한 특징과 장점들로 인하여 전 세계의 다양한 산업군에서 클라우드 서비스 도입 및 전환이 빠르게 확산하는 추세이다. 이러한 멀티클라우드 기반의 서비스가 확산함에 따라 보안 취약성 또한 증대되고 있어 클라우드 컴퓨팅 서비스에서의 데이터 유출 사고도 증가할 것으로 전망되고 있다. 이에 본 연구에서는 데이터 보안이 강화되면서도 클라우드 구축 비용을 절감할 수 있는 AWS Well-Architected 기반의 보안 아키텍처 구성방안을 제안한다. 제안하는 AWS 클라우드 보안 아키텍처는 개인정보 처리 시 요구되는 보안 항목을 충족하는 Standard 보안 참조모델 및 비용 효율화를 고려한 Shared Security 참조모델로 설계하였다. 본 연구에서 제안하는 AWS 보안 아키텍처는 안전하고 신뢰성 높은 AWS 클라우드 시스템을 구성하는 기업과 기관에 도움을 줄 수 있을 것으로 기대한다.

주제어 : AWS 보안, 클라우드, 아키텍처, 데이터 보안, 보안 위협

Abstract Recently, due to the many features and advantages of cloud computing, cloud service is being introduced to countless industries around the world at an unbelievably rapid pace. With the rapid increase in the introduction of multi-cloud based services, security vulnerabilities are increasing, and the risk of data leakage from cloud computing services are also expected to increase. Therefore, this study will propose an AWS Well-Architected based security architecture configuration method such as AWS standard security architecture, AWS shared security architecture model that can be applied for personal information security including cost effective of cloud services for better security in AWS cloud service. The AWS security architecture proposed in this study are expected to help many businesses and institutions that are hoping to establish a safe and reliable AWS cloud system.

Key Words : AWS Security, Cloud, Architecture, Data Security, Security Threats

1. 서론

급속한 ICT 기술의 발전으로 인하여 데이터 종류의 다양화와 데이터 규모의 확대는 인공지능, 빅데이터, 사물인터넷 등의 기술을 기반으로 4차 산업혁명 시대의 도래를 가속화 하였다. 이에 따라 산업현장에서 대량의 데이터 활용이 증가하면서 안전하고 신뢰받는 환경의 필요성이 요구되고 있다.

정보통신 자원의 유연한 사용을 가능하게 하는 클라우드 컴퓨팅 기술은 데이터의 수집과 분석, 데이터 가용성 확보, 데이터 활용 극대화 등을 위한 투입비용 대비 효율적인 서비스를 제공하기 때문에 안전성이 보장

*This article is extended and excerpted from the conference paper presented at ICSMB 2021
*Corresponding Author : Yong-Joon Lee(2020032@kdu.ac.kr)
Received May 23, 2021
Revised June 6, 2021
Accepted July 20, 2021
Published July 28, 2021

된 컴퓨팅 환경에서의 효과적인 데이터 활용을 위하여 많은 기업은 클라우드 컴퓨팅 기술 도입 및 전환을 적극적으로 검토하고 있다[1,2]. 그러나 클라우드 컴퓨팅 서비스 도입 및 전환이 확산함에 따라 보안 취약성 또한 증가하고 있으며 이에 따른 데이터 유출 역시 증가할 전망이다[3,4]. 또한 최근 빅데이터 분석을 위한 데이터의 활용이 보편화되면서 개인정보, 건강정보, 위치정보 등 의미 있는 데이터의 보유 및 처리 관점에서 보안의 필요성이 요구되고 있다. 즉, 데이터의 소유권은 정보 주체에게 있지만, 데이터의 수집, 분석 및 활용은 클라우드 컴퓨팅 환경에서 이루어지고 있는 상황에서 클라우드 기반 인프라와 서비스 프로그램이 보안에 취약할 경우 데이터 보안 문제가 발생할 수 있으므로 보안에 대한 고려가 필요하다.

AWS 클라우드에서는 Well-Architected Framework에 기반한 참조모델을 제시하고 있고 보안 영역에 대한 요건을 포함하고 있으나, 개인정보 처리 시 요구되는 보안 요구사항을 충족하기 위하여 보안 관점에서 강화 및 개선이 필요한 부분이 존재하며 보안 아키텍처 구성 시 비용 효율화 관점에서도 개선될 필요성이 있다. 이에 따라 본 연구에서는 개인정보 처리 시 요구되는 보안 항목을 충족하는 AWS Standard 보안 아키텍처 참조모델 및 비용 효율화를 고려한 AWS Shared Security 아키텍처 참조모델을 제안한다.

2. 관련 연구

2.1 클라우드 서비스 모델

NIST(National Institute of Standards and Technology)에서 정의된 모델에서는 클라우드 컴퓨팅을 최소한의 관리나 서비스 제공자의 상호 작용만으로 컴퓨팅 시스템을 구성하는 자원들을 신속하고 편리하게 제공받을 수 있는 서비스로 정의한다[5]. 클라우드 서비스 모델은 일반적으로 서비스 유형에 따라 IaaS, PaaS, SaaS 3가지로 분류할 수 있다[6,7].

IaaS(Infrastructure-as-a-Service)는 서버, 스토리지, 네트워크 및 보안 등의 물리적인 컴퓨팅 인프라를 사용자에게 사용량 기반으로 제공하는 서비스이다. PaaS (Platform-as-a-Service)는 사용자가 자신의 Application 개발이나 테스트 및 실행에 필요한 운영체제와 같은 컴퓨팅 플랫폼을 클라우드 서비스 형태로 제공하는 것이 목적이며, SaaS(Software-as-a-Service)는 표준화된 Application 프로세스 및 소프트웨어를 클라우드 서비스 형태로 제공하는 데 목적이 있는 서비스 모델이다[8].

2.2 클라우드 컴퓨팅 보안 위협

클라우드 컴퓨팅은 가상화 기술의 적용, 자원의 공유, 정보의 외부 위탁, 다양한 단말 접속환경 등의 특징을 가지고 있으며 이러한 특징에 따라 클라우드 컴퓨팅에 대한 보안 위협도 다양하게 발생할 수 있다.

CSA(Cloud Security Alliance)에서는 매년 Cloud 환경에서의 보안 위협을 지속해서 발표하고 있으며 2019년에는 데이터 유출, 잘못된 설정&변경관리, 보안 아키텍처 미흡, ID/자격증명/Key 관리 미흡, 계정 Hijacking, 내부자 위협, 불안전한 API, 취약한 제어 영역, Application Structure 실패, 클라우드 가시성 제한, 클라우드 서비스 오용과 같은 11개의 클라우드 컴퓨팅 보안 위협이 있음을 발표하였다[9,10]. 이처럼 클라우드 서비스의 도입 및 이용이 활성화됨에 따라 클라우드 컴퓨팅 보안 위협도 관리적, 기술적 범위에서 점진적으로 증가하고 있으며 클라우드 컴퓨팅 환경에서 새롭게 추가된 보안 위협 또한 발생하고 있음을 알 수 있다. CSA의 최근 발표 자료에 따르면 클라우드 컴퓨팅 보안 위협 요소는 시스템, 프로그램 취약성 등 기술적 문제보다는 내부자의 불충분한 관리와 부주의 등 기술 외적인 문제가 더욱 중요한 요소임을 지적하고 있다. 이는 기술적 보안 위협에 대한 대응과 함께 내부자들에 대한 지속적인 보안 인식 제고가 매우 중요한 부분임을 또한 알 수 있다.

3. AWS 보안 아키텍처

3.1 AWS Well-Architected Framework

AWS에서는 Well-Architected Framework에 기반한 다양한 참조 아키텍처를 제시하고 있다. AWS Well- Architected Framework는 '운영 우수성', '보안', '시스템 안정성', '성능 효율성', '비용 최적화'와 같이 5개 영역을 고려하여 참조 아키텍처를 제시하고 있으며, AWS 클라우드 컴퓨팅 환경에서도 보안은 시스템 설계 시 반드시 고려해야 하는 사항임을 알 수 있다. 5개 영역 중 '보안' 영역은 Table 1에서와같이 'ID 및

접근관리', '탐지 제어', '인프라 보호', '데이터 보호', '사고 대응'과 같이 총 5개의 보안 항목으로 구성되어 있다.

Table 1. Security in AWS Well-Architected Framework

Security Area	AWS Service
[1] ID&Access Management	IAM
[2] Detective Controls	CloudTrail, FlowLogs
[3] Infrastructure Protection	Shield, SG, WAF, IDS
[4] Data Protection	KMS, ACM
[5] Incident Response	Security Hub

'ID 및 접근관리' 영역에서는 AWS 서비스 및 자원에 대한 접근관리를 위해 IAM을 통한 역할 및 권한 그룹의 설정 방안을 제시하고 있고, '탐지 제어' 영역에서는 AWS 환경 내 로그 가시성과 책임 추적성 확보를 위하여 CloudTrail, VPC Flow logs, Config 등을 통해 구현방안을 제시하고 있다. '인프라 보호'는 전통적인 On-Premise 환경에서의 보안과 같이 네트워크 보안, 서버 보안 등에 대하여 Security Group, AWS WAF, Inspector 등을 통한 구현방안을 제시하고 있으며, '데이터 보호' 영역에서는 RDS, S3 등 저장소에 대한 암호화와 AWS Certificate Manager를 통한 전송구간 암호화 방안에 대하여 제시하고 있다. 마지막으로 '사고 대응' 영역에서는 AWS 환경에서 발생하는 보안 위협을 모니터링하고 탐지 시 대응 프로세스를 갖추는 방안에 대하여 제시하고 있음을 볼 수 있다.

3.2 AWS 보안 아키텍처 구성방안

Well-Architected Framework 기반으로 AWS에서 제시하고 있는 보안 아키텍처는 기본적인 Native 서비스 구성으로 제시되어 있으며, 개인정보 처리 시 국내 법규 및 규제에서 제시하는 보안 요건을 충족하기 위해서는 AWS 보안 Native 서비스에 대한 추가 반영이 필요하고 또한 일부 보안 영역에서는 Native 서비스 적용 시 한계점, 그리고 이를 충족 및 대체할 수 있는 3rd-Party 적용 영역에 대한 고려가 필요하다. 또한 3rd-Party 적용 시 여러 클라우드 서비스 도입 및 전환 비용 효율화 관점에서도 고려할 필요성이 있다. 이를 위하여 아래 Table 2와 같이 Standard 보안 아키텍처 참조모델과 Shared Security 참조모델을 제시한다.

Table 2. Security Architecture Reference Model

Model Type	Description
Standard	- Regulation based Configuration
Shared Security	- Cost Effective Configuration

Standard 보안 아키텍처 참조모델은 개인정보를 처리하는 데 요구되는 법규, 규제 및 대내/외 보안인증을 위한 구성방안을 제시하고, Shard Security 아키텍처 참조모델은 보안 비용 효율화 관점을 고려한 구성방안을 제시한다.

4. AWS 보안 아키텍처 구성방안

4.1 Standard 보안 아키텍처 구성

Standard 보안 아키텍처 참조모델은 AWS Well-Architected Framework 상의 보안 항목에서 기본적으로 제시되고 있는 AWS Native 서비스를 포함하고 법규 준수 및 대/내외 인증을 위하여 AWS Shield Advanced, CloudHSM, Security Hub, Audit Manager, Detective, Macie, Inspector, Artifact 서비스를 추가로 고려하여 Fig. 1과 같이 구성하였다.

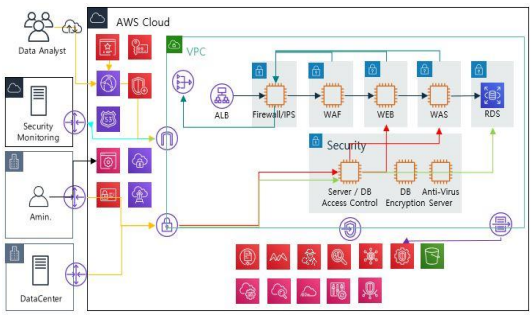

Fig. 1. Standard Security Architecture

Standard 보안 아키텍처 참조모델은 AWS Well-Architected Framework에서 제시하는 5가지 보안 항목 기반으로 법규 및 규제에서 요구하는 수준을 충족할 수 있도록 다음과 같이 설계하여 제시하였다.

ID 및 접근관리 영역에서는 AWS 내의 모든 자원에 대한 접근 가능한 ID의 생성과 권한관리는 AWS IAM을 통하여 이루어진다. AWS는 기존 On-Premise에서 데이터센터에 물리적으로 출입하여 서버의 반입과 반출에 해당하는 과정을 AWS 관리 콘솔을 통해 온라인

상에서 모두 이루어지게 되므로 IAM을 통한 자원에 대한 접근관리가 매우 중요하다고 할 수 있다. 그러므로 가장 우선하여 비밀번호 규칙과 MFA(Multi-Factor Authentication) 적용 등 AWS에서 제시하는 계정보안 설정을 적용하고, 이후 IAM 사용자를 생성하여 사용자 그룹에 업무 역할에 맞는 권한을 할당하는 등의 계정보안을 설정하는 것이 중요하다. 이렇게 생성된 IAM 사용자를 통하여 AWS 내 자원 관리를 수행해야 하며, 모든 권한을 보유한 루트 계정은 사용하지 않도록 관리한다.

탐지 제어 영역에서는 IAM 사용자가 AWS 관리 콘솔, CLI 등을 통하여 AWS 환경의 자원을 제어하는 모든 이력은 CloudTrail에 보존된다. 기본적으로 90일간 보존되기 때문에 Regulation 정책 준수를 위해서는 별도의 S3에 해당 로그를 보존하도록 추가 설정이 요구된다. 그리고 AWS VPC 내에서 발생하는 모든 네트워크 트래픽 로그는 VPC Flow logs를 통해 보존할 수 있다. VPC Flow logs는 기본적으로 비활성화되어 있으므로 별도 활성화 설정이 필요하고 이를 통해서 GuardDuty와 같은 지능형 위협 탐지 서비스에서 AWS 환경에서의 보안 위협을 탐지할 수 있다. 또한 AWS와 같은 클라우드 환경에서는 자원의 탄력적인 운영이 가능하므로 자원의 생성, 삭제 등의 변경이 빈번하게 발생하는데 계획되지 않은 자원의 변경이나 비인가자에 의한 자원 변경 등에 대해 인지하고 추적하기 위해 AWS Config 서비스 적용을 통해서 자원 변경이력을 추가로 확보할 수 있다.

인프라 보호영역은 웹 서비스 접근에 대한 보호와 데이터베이스 접근에 대한 보호 관점에 대한 고려가 필요하다. 웹 서비스로 접근하는 트래픽에 대해서 CloudFront의 Geo-Blocking 기능을 통해서 웹 서비스에 접근 가능한 국가를 제한하여 보안 위협을 최소화하고, AWS Shield 및 Shield Advanced 서비스를 통해 DDoS 공격에 대한 트래픽을 방어한다. 이후 침입탐지시스템과 웹 방화벽을 활용하여 유해 트래픽과 웹 취약점에 대한 공격을 방어하고 해당 보안솔루션의 보안로그는 관제시스템과의 연동을 통해 모니터링을 수행하고 위협에 대응할 수 있도록 구성한다. 또한 Inspector를 통해서 시스템의 취약점을 진단하고 백신을 통하여 악성코드 감염으로부터 상시로 시스템을 보호하도록 구성한다.

데이터 보호를 위해서는 전송 시 암호화와 저장 시 암호화 적용이 필요하다. 전송 시 암호화는 End-User와 웹 서버 간의 인터넷망 통신 구간을 암호화하는 것으로 AWS Certificate Manager의 SSL 인증서를 ELB 혹은 웹 서버에 적용하여 구성한다. 저장 시 암호화는 중요한 데이터가 보존되는 RDS, S3와 같은 데이터 저장소에 KMS에서 발급한 Customer Managed Key를 통하여 저장소 내 데이터를 암호화하고 해당 키를 주기적으로 변경할 수 있으며, 필요할 때 하드웨어 보안 모듈을 통한 암호화 키 관리 보안 강화를 위하여 CloudHSM 서비스 구성이 가능하다.

사고 대응을 위해서는 AWS 환경 내에 보안 위협에 대해서 상시적인 모니터링을 위해 GuardDuty 서비스를 활성화하고 SNS 연동을 통해 발생하는 이상징후에 대해 보안담당자가 인지할 수 있도록 Alert 설정 적용이 요구된다. 또한 침입탐지시스템, 웹 방화벽 대상으로 보안관제를 수행함으로써 보안 위협 모니터링 및 대응체계 수립이 가능하도록 구성한다. 또한 Security Hub, Audit Manager 서비스를 활용하여 보안 Alert, 규정 준수 등 현황이 통합된 대시보드를 통하여 보안 모니터링 자원을 효율화하고 Detective, Artifact 서비스를 통하여 AWS Account 내에서 발생한 보안 이슈의 자동화된 원인 분석을 통하여 보안 위협을 제거하며 Macie 서비스를 통하여 RDS, S3 내 저장된 개인정보 등에 대한 현황을 주기적으로 점검할 수 있도록 구성한다. 이처럼 5가지 보안 항목 기준으로 추가 구성이 필요한 Native 서비스까지 고려하여 보안 아키텍처를 구성한 후에는 AWS Native 서비스 적용 시 보안 관점에서의 적정성 및 한계점에 대한 검토가 필요하다.

Domain	Security Area	AWS Native	Verification
N/W	DDoS	Shield	○
	Firewall	SG/NACL	○
	IDPS	N/W F/W	X
	SSL-VPN	Client VPN	△
DB/Storage	DB Access Control	-	X
	Data Encryption	KMS	△
Server	Server Access Control	Session Manager	△
	Anti-Virus	-	X
Application	Web Firewall	AWS WAF	△
	Transmission Encryption	ACM	○

Fig. 2. AWS Native Service Verification

Fig. 2는 N/W, DB/Storage, Server, Application 각각의 영역 기준으로 제시하고 있는 AWS Native 서비스 대상으로 법규 및 규제에서 요구되는 수준의 충족 여부의 검토 결과를 나타낸 것이다.

AWS Native 서비스 중에서 Shield, Security Group 및 NACL, ACM 서비스는 별도 고려사항 없이 보안 아키텍처 구성이 가능하다. Client VPN, KMS, Session Manager, AWS WAF 서비스를 활용한 보안 아키텍처 구성 시에는 다음과 같은 사항을 고려하여야 한다. Client VPN 서비스는 자체적으로 MFA를 지원하지 않으므로 IAM 등의 서비스와의 연동을 통하여 MFA를 구성하여야 하고, KMS는 블록 암호화와 키 관리 기능을 제공하지만, 별도 필드 암호화 기능을 지원하지 않으므로 해당 요건이 발생하면 3rd-Party 적용을 고려하여야 하며 Session Manager는 Windows 서버 대상으로는 RDP 접속이 불가함을 고려하여 구성하여야 한다. 또한 AWS WAF는 관리형 Rule-set이 제공되기는 하지만 기존 On-Premise 대비 관제 수준이 충분하지 않은 이슈가 존재함을 고려하여야 한다. Network F/W IPS 서비스 및 DB 접근통제, Anti-Virus 영역 대상으로는 3rd-Party 적용이 필요하다. Network F/W IPS 서비스는 기본으로 제공되는 침입탐지 Rule-set이 없고 국내 보안관제 수행이 어려운 관계로 3rd-Party 적용이 필요하지만, 신규 출시된 서비스임을 고려하여 추후 관리형 Rule-set 제공, 보안관제 수행이 가능해지는 시점에서는 보안 아키텍처 구성이 가능할 것으로 판단된다. DB 접근통제를 위한 AWS Native 서비스는 제공되지 않으므로 3rd-Party 적용이 필요하다. 다만, 정형 DB의 경우에는 법규 및 규제에서 요구하는 Logging 시 DB 성능저하 이슈를 보완할 수 있다면 Client VPN, IAM 구성을 통하여 AWS Native 기반의 DB 접근통제 구성이 가능하다. Anti- Virus를 위한 AWS Native 서비스 또한 제공되지 않으므로 3rd-Party 적용이 필요하다. 일부 Windows 서버 대상으로는 Microsoft Defender 서비스 구성이 가능하지만, 통합관리 및 모니터링이 기능이 제공되지 않으므로 보안 아키텍처 구성으로는 적합하지 않은 것으로 판단된다.

Fig. 3은 Anti-Virus 영역을 제외하고 Network F/W IPS 서비스 및 DB 접근통제 영역까지 모두 AWS Native 서비스로 구성하여 제시한 AWS Native 기반의 Standard 보안 아키텍처 참조모델로써, 3rd-Party 구성 대비 S/W 라이선스, S/W 설치형 VM 비용 등의 관점에서 비용 절감 효과 및 빠른 클라우드 서비스 도입 및 전환이 가능해질 것으로 판단된다.

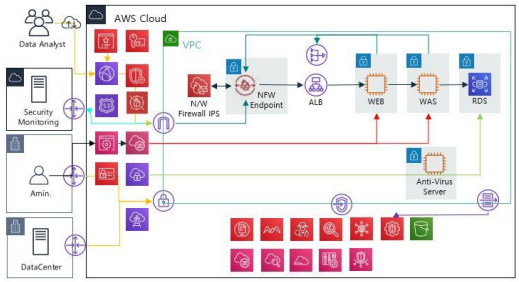

Fig. 3. Standard Security Architecture – Native Configuration

4.2 Shared Security 아키텍처 구성

Shared Security 아키텍처 참조모델은 다양한 클라우드 서비스 구성 환경에서 보안이 구성된 AWS Account를 별도 구성하여 비용 절감 및 보안체계 통합관리 방안으로 활용할 수 있도록 구성하였다.

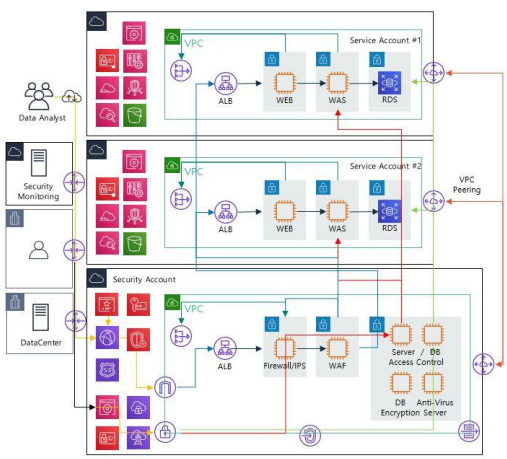

Fig. 4. Shared Security Architecture

Fig. 4에서 제시된 Shared Security 아키텍처는 별도의 AWS Security Account를 구성하여 앞에서 제시한 Standard 보안 아키텍처 참조모델 수준의 AWS Native 서비스 및 3rd-Party 솔루션을 적용하고 클라우드 서비스를 제공하는 여러 Service Account와 VPC Peering으로 연동하여 보안 서비스를 제공하는

참조모델이다. Security Account 구성을 통하여 Shared 서비스가 제공되는 참조모델이므로, 클라우드 서비스를 제공하는 Service Account에서는 별도의 보안솔루션 적용, 운영 및 보안관제 수행이 필요하지 않으며, 각각의 클라우드 서비스 구성 시 요구되었던 보안 요건에 대한 구성이 필요하지 않으므로 이에 따른 클라우드 구축 및 전환 시 비용을 절감할 수 있다. 또한 Security Account를 통하여 보안체계를 통합으로 관리할 수 있으므로 보안 운영 및 관제 효율화 관점에서도 보안 수준 제고가 가능할 것으로 판단된다.

Shared Security 아키텍처 구성 시에도 Fig. 5와 같이 앞에서 제시한 AWS Native 기반의 보안 아키텍처 구성을 적용할 수 있고 이처럼 구성하면 추가적인 비용 절감 효과를 얻을 수 있으며, 다수의 Service Account와 Peering으로 구성되는 경우 Peering 정책과 성능의 효율성을 위하여 Transit Gateway를 활용하여 Shared Security 아키텍처 구성이 가능하다.

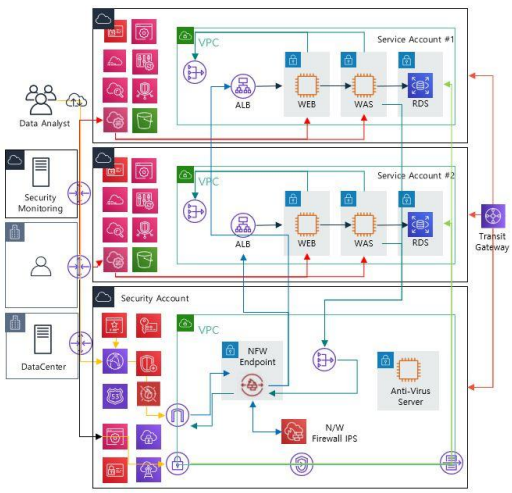

Fig. 5. Shared Security Architecture - Native Configuration

5. 결론

최근 클라우드 컴퓨팅 서비스 도입이 확산하고 있음에 따라 보안 취약점 또한 증가하고 있고 클라우드 컴퓨팅 서비스에서의 보안사고 또한 증가할 것으로 전망되고 있어 본 연구에서는 가장 많이 사용하고 있는 AWS 클라우드 서비스에서의 보안 아키텍처 참조모델을 제시하였다. 이를 위해 관련 연구로서 클라우드 서비스 모델 및 클라우드 컴퓨팅 보안 위협에 대하여 살펴보았다. 이후 관련 연구를 참조하여 AWS Well-Architected Framework 상의 보안을 고려한 AWS 보안 아키텍처 참조모델을 구성하여 제안하였다.

AWS 클라우드에서 가용한 모든 보안을 구성하고 개인정보 처리를 위한 법규 및 규제를 준수하는 수준의 Standard 보안 아키텍처 참조모델을 제시하였고, 보안 비용 절감 및 보안체계 통합관리 방안으로 활용 가능한 Shared Security 아키텍처 참조모델을 제시하였다. 제안하는 보안 아키텍처 참조모델은 AWS Well-Architected Framework 상의 '보안' 영역에서 요구하는 'ID 및 접근관리', '탐지 제어', '인프라 보호', '데이터 보호', '사고 대응'의 5가지 보안 요건을 충족하는 수준으로 설계하여 제시하였다.

AWS 클라우드 환경 외에도 Azure, GCP, NCP 등 다양한 멀티클라우드 환경에서 데이터 활용 기반 플랫폼이 더욱 활성화될 것으로 전망되며, 이에 따라 데이터 유형에 따른 법규 및 규제 기반에서 데이터 활용성 및 보안에 대한 딜레마는 더욱더 심화할 것이고 이에 따라 데이터 보호를 위한 새로운 컴퓨팅 시스템 디자인에 대한 사회적/기술적 요구도 더욱 증대될 것으로 판단된다.

본 연구에서 제안한 AWS 보안 아키텍처 참조모델이 향후 안전하고 신뢰성 높은 AWS 클라우드 시스템을 구축하고자 하는 기업과 기관에 도움이 되기를 기대한다.

REFERENCES

[1] T. Wang et al. (2016). Fog-based storage technology to fight to fight with cyber threat. *Future Generation Computer Systems, 83*, 208-218. DOI : 10.1016/j.future.2017.12.036

[2] Multi-Cloud Blog. (2020). *SaaS vs PaaS vs IaaS: What's the difference and how to choose.* Accessed Time (Online). https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-what's-difference-and-how-to-choose

[3] ENSI-MARIA. (2017). *IaaS, PaaS, SaaS - What do they mean?*, Cloud on move (Online). http://cloudonmove.com/iaas-paas-saas-what-do-they-mean

[4] Cloud Security Alliance. (2016). *Cloud*

Computing Top Threats in 2016. The Threacherous 12.

[5] J. H. Jeong. (2017). Current status and challenges of cloud computing, *INARS issue report, 313,* 17-21.

[6] S. H. Cho. (2018). *A Study on Security Management Method for Hybrid Cloud Computing Environment.* Master's Thesis, Graduate School of Dongguk University, Seoul.

[7] Cloud Security Alliance. (2019). *Top Threats to Cloud Computing in 2019*. The Egregious 9.

[8] C. J. Lee. (2017). *A Study on Security Requirements for Privacy in a Home Cloud Environment.* Master's Thesis. Graduate School of Soon Chun Hyang University, Asan.

[9] Y. G. Lee. (2019). *A Study on Improvement of Cloud Security Assurance Program.* Master's Thesis, Graduate Schoolof Dongguk University, Seoul.

[10] P. Mell & T. Grance. (2011). *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology, U.S. Department of Commerce Version 15.

박 세 준(Se-Joon Park) [정회원]

· 1996년 2월 : 숭실대학교 수학과 (이학사)
· 1998년 2월 : 숭실대학교 컴퓨터 공학과(공학석사)
· 2004년 8월 : 숭실대학교 컴퓨터 공학과(공학박사)
· 2006년 1월 ~ 현재 : SK 정보보호담당 수석연구원
· 관심분야 : 개인정보보호, 인공지능 보안, 정보보호
· E-Mail : sjoon0912@naver.com

이 용 준(Yong-Joon Lee) [정회원]

· 2005년 2월 : 숭실대학교 컴퓨터 학과(공학박사)
· 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구위원
· 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
· 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수
· 관심분야 : 인공지능 보안, 국방보안, 해킹 보안
· E-Mail : 2020032@kdu.ac.kr

박 연 출(Yeon-Chool Park) [정회원]

· 2004년 2월 : 숭실대학교 컴퓨터 학과(공학박사)
· 2005년 4월 ~ 2009년 3월 : 성균관대학교 ISRI 연구교수
· 2009년 5월 ~ 2010년 6월 : 스웨덴Umea Univ. Post-Doc.
· 2011년 4월 ~ 2013년 2월 : 프랑스 Pascal Institute Post-Doc.
· 2013년 9월 ~ 현재 : LG전자 CTO 책임연구원
· 관심분야 : 컴퓨터비전, 로봇비전, 인공지능
· E-Mail : fearhope@gmail.com