클라우드 보안 인증기술 동향 분석

김구민, 김경백

전남대학교 정보보안협동과정

Trend Analysis of Cloud Security Authentication Technology

Gu-min Kim, Kyungbaek Kim

Interdisciplinary Program of Information Security, Chonnam National University

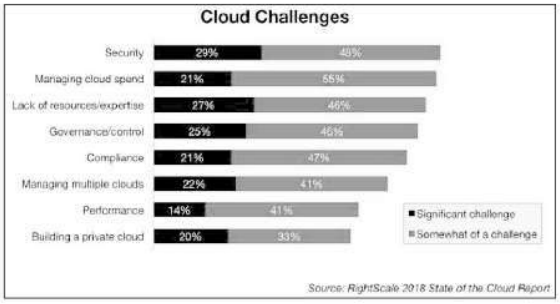
요 약

ICT 기술의 발달과 함께 COVID-19가 전 세계적인 펜데믹으로 확대됨에 따라 온라인 기반의 서비스와 소비가 더욱 증가하고 기업에서는 디지털 전환이 가속화되면서 클라우드는 공공, 기업, 사회 시스템의 연속성을 보장하는 효과적인 수단으로 재조명받고 있다. 하지만 클라우드 성장과 함께 클라우드를 목표로 하는 보안 위협도 꾸준히 증가하고 있어 안전하고 효율적인 클라우드 활용을 위한 보안 기술 연구가 필수적이다. 이 논문에서는 클라우드 보안을 위한 인증기술 동향을 정리하고 분석한다.

I. 서론

클라우드 컴퓨팅은 IT 리소스를 인터넷을 통해 온디맨드로 제공하고 사용한 만큼만 비용을 지불하는 형태의 기술을 말한다. 서비스 간 또는 서비스와 기능 간 결합 등을 통해 다양한 서비스가 파생될 수 있는 매개체로서 서비스 제공과 비용의 효율성을 위해 많은 기업·기관들이 클라우드 환경을 활용하려 시도하고 있다.

하지만 사용자의 컴퓨터 자원을 제공자가 일괄적으로 관리하는 클라우드의 특성상 클라우드 환경에서 정보 유출이 발생할 경우 기존의 서비스 제공 환경보다 더 큰 피해가 발생하기 때문에 보안의 필요성이 더 부각되고 있다. 이러한 이유로 미국의 클라우드 컴퓨팅 관리 회사인 RightScale이 실시한 설문조사 결과에 따르면 기업들은 클라우드 도입 시 보안 이슈를 가장 큰 어려움이라 생각하고 있다 [1].



[그림 1] 클라우드 도입시 겪는 어려움

클라우드 컴퓨팅 환경에서의 보안 취약점은 꾸준히 발견되고 있으며 해결을 위한 연구들이 활발히 진행되고 있다. 이 논문에서는 인증 보안과 관련된 기술 동향을 살펴본다.

2절에서 클라우드 컴퓨팅 모델의 종류와 주로 위협이 되는 이슈를 확인하고 3절에서 클라우드 환경에서의 보안 문제를 해결하기 위한 인증 기술의 연구 동향을 살펴본다. 4절에서 전체적인 정리 및 논의로 논문을 마무리한다.

II. 클라우드 컴퓨팅 개요

클라우드 컴퓨팅은 클라우드 컴퓨팅 플랫폼에서 접근할 수 있는 특정 유형의 서비스를 의미하는 서비스 모델과 클라우드 인프라의 위치 및 관리를 의미하는 배치 모델로 분류된다 [2].

2.1 서비스 모델

서비스 모델은 Legacy 환경에서 사용자에게 제공하는 컴퓨팅 자원의 범위에 따라 IaaS, PaaS, SaaS로 나눌 수 있다.

IaaS(Infrastructure as a Service)는 서버, 네트워크, OS, 스토리지를 제공하고 관리하는 가상화 서비스로 고객들은 서버와 스토리지를 접근할 수 있지만 사실상 클라우드 내 가상 데이터 센터를 통해 리소스를 전달받는 형태이다. IaaS는 기존 데이터 센터에서 제공받던 물리적 자산을 완벽하게 가상화하여 제공하기 때문에 서버 사양의 변경 등 물리적 자산의 수정이 필요한 경우 기존 방식에 비해 훨씬 빠른 대응이 가능하다.

PaaS(Platform as a Service)는 OS, 미들웨어, 런타임과 같은 소프트웨어 작성을 위한 플랫폼을 가상화하여 제공하는 서비스이다. 사용자는 운영체제, 소프트웨어 업데이트, 저장소 또는 인프라에 대한 관리 없이 소프트웨어 개발에 집중할 수 있다.

SaaS는 기존 온프레미스 방식과 다르게 소프트웨어와 데이터를 제공하고 관리하여 개별 컴퓨터에 응용 프로그램을 다운로드·설치할 필요가 없다. SaaS는 데이터, 미들웨어, 서버 및 스토리지 등 모든 잠재적인 기술적 문제를 관리하기 때문에 사용자의 관리적 부담이 적다.

2.2 배치 모델

배치 모델은 사용 대상과 배치 형태에 따라 Public, Private, Community, Hybrid 클라우드로 나눌 수 있다.

Public 클라우드는 서비스 사용 대상의 제한 없이 인터넷망을 통해 불특정 다수에게 서비스를 제공하는 형태이다. 모든 주체가 클라우드 서비스를 이용할 수 있고 적은 비용으로 높은 서비스를 제공할 수 있다.

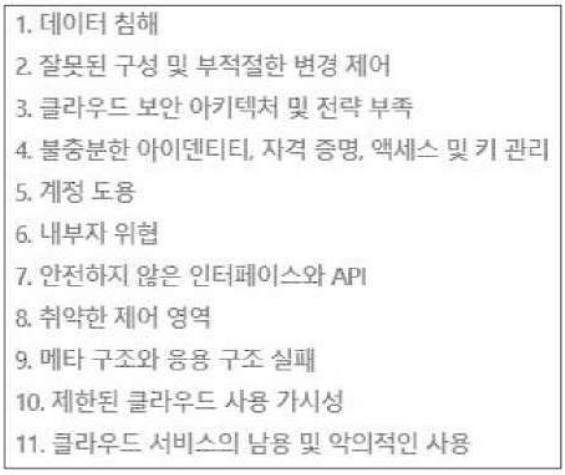
Private 클라우드는 특정 조직이나 기업 내부자 등에게 클라우드 서비스를 구성하여 제한적인 서비스를 제공하는 형태이다. Public 클라우드보다 많은 제어 권한과 우수한 보안을 제공한다.

Community 클라우드는 문제사항을 공유하는 (예: 임무, 보안 요구 사항, 정책 및 준수 고려 사항) 소비자의 특정 커뮤니티에서 독점적으로 사용할 수 있도록 제공되는 형태이다.

Hybrid 클라우드는 상기 클라우드의 조합으로 구성된 형태로 상기 클라우드들의 단점은 보완하고 장점은 살릴 수 있는 유동적인 형태이다.

2.3 클라우드 보안 취약점

CSA의 클라우드 위협 보고서에 의하면 클라우드 환경에서의 주요 취약점을 11가지로 꼽았다 [3]. 서비스 거부, 공유 기술 취약성 및 CSP(Cloud Service Provider) 데이터 손실, 시스템 취약성과 같은 문제는 올해 보고서에서 제외되었다.



[그림 2] 클라우드 보안 주요 취약점

더불어 2020 CSA 설문조사 응답자의 94%는 인적 권한 및 권한 관리를 가장 큰 과제로 생각하고 있으며 응답자의 77%는 시스템 권한 및 권한 관리만큼이나 중요한 문제로 간주하고 있다는 결과로 보아 안전한 인증, 권한부여, 접근

제어를 수행하는 IAM(Identity Access Management) 기술은 이러한 취약점들 중 많은 부분을 보완하는데 반드시 필요한 필수 보안 기술로 분석된다. 이 논문에서는 안전한 클라우드 운영 및 관리를 위한 인증기술 및 동향에 대해 정리하고 분석한다.

III. 클라우드 보안 인증기술 동향

3.1 암호화를 통한 인증기술

John과 Dirksen은 JavaScript에서 제공하는 애플리케이션을 통해 공격자가 클라이언트 측 컴퓨팅에 대한 향상된 제어가 가능함을 이유로 기존 개인정보보호 애플리케이션이 웹 기반 클라우드 애플리케이션에 그대로 적용되기 어려운 점을 지적하였다. 이를 위해 클라이언트 측 암호화된 사용자 데이터와 잠재적으로 신뢰할 수 없는 자바스크립트 사이에 강력한 격리계층을 제공하여 웹 애플리케이션을 개발하는 동시에 현재 클라이언트 측 개발 관행과 완전한 상호 운용성을 유지할 수 있는 CryptoMembranes를 제안하였다 [4].

CDN(Content Distribution Network)에서 클라우드 서비스를 활용할 때 신뢰성 있는 서비스를 제공하기 위해 암호통신 프로토콜로 TLS를 사용하는 경우가 많다. 그러기 위해서는 사용자와 종단 간 유효한 TLS 연결을 설정하기 위해 자신을 원본 서버로 인증해야 하는데 표준 TLS에서는 서버의 비밀 키에 접근해야 하므로 인증 위임 기법이 필요하다. Alber 등은 키 공유가 필요하지 않은 신원 기반 서명 기법을 적용한 단기 위임 기법을 제안하였다 [5]. 순방향 보안(Forward-Secrecy)을 통해 서버의 비밀키가 누출되는 경우에도 기존 위임의 유효성을 유지할 수 있으며 구현을 통해 일반적인 네트워크 통신보다 통신 오버헤드가 적음을 입증하였다.

A.Sarana, R.Naresh는 모바일 결제 수단에서 지불 신뢰도와 고객 기밀성은 보안에 있어 사용자에게 불안을 갖게 해준다는 점을 지적하였다. 이를 위해 키 분배 방식을 이용하여 인증서 없는 프록시 재서명 시스템을 기반으로 모바일 결제를 위한 클라우드 기반의 인증방법을 제안하였다 [6]. 구현을 통해 더 작은 양의 데이터를 사용하여 스토리지 복잡성을 달성함으로써 클라우드에서 소스가 부족한 스마트 모바일 환경에 합리적이고 빠른 처리 시간을 보장함을 보였다.

3.2 신원 중심의 인증 기술

Jay Chen은 RSAConference2021에서 신원 증명 보안을 강화한 모델을 제안하였다 [7]. IAM 역할에 익명 액세스를 부여하지 않음으로써 역할 이름을 추측하기 어렵게 하여 IAM 역할 신뢰 정책을 강화하였다. 보안 주체가 작업할 수 있는 역할 및 서비스에 대해 제한을 적용하여 PassRole 권한을 강화하였고 모든 클라우드 리소스에 대해 기본적으로 액세스 제한을 적용함으로써 절대적으로 필요한 권한만 부여하였다. 더불어 모든 사용자 및 IAM 역할에 대해 MFA(Multi-Factor Authentication)를 활성화하고 자격증명 교체 자동화와 지속적인 모니터링을 적용하였다.

Teena Joseph 등은 바이오 정보의 특장점을 융합한 다중 인증 시스템을 제안하였다 [8]. 각 특성은 전처리, 정규화 및 특징 추출과 같은 이미지 처리 기술의 절차를 거쳐 추출된 특성에서 특성을 2단계로 융합하여 고유한 비밀 키를 생성한다. FAR(False Acceptance Rate) 및 FRR(False Rejection Rate) 메트릭을 이용하여 시스템의 견고성을 측정하였고 AES, DES 및 Blowfish와 같은 세 가지 표준 대칭 암호화 알고리즘을 사용하여 성능 평가를 진행하여 데이터에 대한 강화된 보안 및 액세스 제어 제공을 입증하였다.

3.3 인증 프로토콜

Masoumeh Safkhani 등은 최근에 제안된 차량용 클라우드 컴퓨팅용 RFID 기반 인증 프로토콜인 RSEAP가 원하는 보안을 제공하지 못하며 태그 및 리더 사칭 공격에 취약함을 지적하였다. 그에 따라 RSEAP 체계의 보안을 개선하기 위해 RSEAP2 라는 개선된 프로토콜을 제안

하였다 [9]. Real-or-Random 오라클 모델 환경에서 암호화 프로토콜 보안 자동화 평가 도구인 Scyter를 사용하여 향상된 안전성과 효율성을 입증하였다.

IV. 결론

이 논문에서는 클라우드 컴퓨팅 서비스의 보안 취약점과 이를 해결하기 위한 다양한 연구 동향을 살펴보았다.

CISCO는 최근 보안 위협 동향에 대해 "공격자는 해킹하지 않고 로그인한다."라고 정의하며 가성비에 민감한 공격자들이 시간과 비용이 많이 드는 APT 공격보다 관리자 계정을 이용해 잠입하는 방식을 선호함을 암시하였다. APT를 위한 전술·전략을 수립하고 공격도구를 개발하는데 들이는 시간과 노력보다 더 적은 투자로 공격을 성공시킬 수 있는 방법이 정상 사용자 계정을 이용하는 것이다. BeyondTrust의 최근 위협 리포트 2019에 의하면 IT·보안 관리자의 64%가 직원 액세스를 잘못 사용하거나 남용하여 침해사고를 겪었다는 결과에 따라 인증 보안에 대한 수요가 계속해서 증가할 것으로 예상된다 [10].

국가적 차원에서도 클라우드 보안 강화 움직임도 빨라지고 있지만 앞서 언급한 바와 같이 많은 기업들이 클라우드 도입 시 보안 이슈를 가장 크게 문제 삼고 있으며 그 이슈 중 인증 보안이 큰 부분을 차지하고 있어 이러한 우려를 해결할 수 있는 대응 방안 및 개선책 마련에 대한 연구가 지속적으로 수행될 필요가 있다.

ACKNOWLEGEMENTS

"이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2019-0-01343)

참 고 문 헌

[1] RightScale, "RightScale 2018 State of the Cloud Report", 2018

[2] NIST, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, 2020

[3] CSA, "Top Threats to Cloud Computing The Egregious 11", 2020

[4] M. Johns, A. Dirksen, "Towards Enabling Secure Web-Based Cloud Services using Clint-Side Encryption," *ACM Cloud Computing Security Workshop*, pp. 67-76, Sep. 2020

[5] L. Alber, S. More, S. Ramacher, "Short-Lived Forward-Secure Delegation for TLS," *ACM Cloud Computing Security Workshop*, pp.

[6] A.Sarana, R.Naresh, "Cloud based efficient authentication for mobile payments using key distribution method", *Journal of Ambient Intelligence and Humanized Computing*, 2021

[7] Jay Chen, "Weak Links in Cloud IAM - Never Trust. Always Verify!", *RSAConference2021*, 2021

[8] Teena Joseph, S.A.Kalaiselvan, S.U.Aswathy, R.Radhakrishnan, A.R.Shamna, "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment", *Journal of Ambient Intelligence and Humanized Computing*, 2021

[9] Masoumeh Safkhani, Carmen Camara, Pedro Peris-Lopez, Nasour Bagheri, "RSEAP2 : An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing", *Vehicular Communications*, 2021

[10] BeyondTrust, "Privileged Access Threat Report 2019", 2019