디지털산업정보학회 논문지 제19권 제1호-2023년 3월
http://dx.doi.org/10.17662/ksdim.2023.19.1.023

클라우드 환경에서의 가시성 제공 방안 연구

김 태 경* · 백 남 균** · 김 정 협***

A Study on the Providing the Visibility in a Cloud Environment

Kim Taekyung · Baik Namkyun · Kim Junghyup

〈Abstract〉

According to the government's plan for cloud conversion and integration of information resources for administrative and public institutions, work is underway to convert administrative and public institutions to the cloud by 2025. In addition, in the private sector, companies in many fields, including finance, are already using cloud services, and the usage is expected to expand more and more. As a result, changes have occurred in security control activities using security systems, it is required to secure visibility for encrypted traffic when building a cloud control environment.

In this paper, an analysis was conducted on the way to provide visibility in the cloud service environment. Ways to provide visibility in the cloud service environment include methods of using load balancer, methods of using security systems, and methods of using equipment dedicated to SSL/TLS decryption. For these methods, Performance comparison was performed in terms of confidentiality, functionality (performance), cost. Through this, the pros and cons of each visibility provision method were presented.

Key Words : Cloud Service, Visibility, SSL/TLS, HTTPs

Ⅰ. 서론

최근에는 대부분의 웹 사이트들은 전송구간 암호화 기능을 제공하기 위해 SSL/TLS(Secure Sockets Layer/Transport Layer Security) 프로토콜을 이용한 HTTPs 서비스를 이용하고 있다[1]. 이 기술은 4계층의 암호화 방식을 이용하여 웹상에서 중요 데이터를 안전하게 보호할 수 있다. 그러나 데이터가 암호화됨에 따라 해커의 공격 데이터 역시 암호화되면서 IDS/IPS, 웹방화벽 등으로 대표되는 네트워크 보안장비들에서도 공격여부를 판단하기 위한 패킷 분석 역시 어렵게 되었다[2].

특히, 이러한 암호화 통신을 이용해 해커가 웹 공격 시도, 데이터 탈취, 명령 전달 등의 악성 행위를 은폐하고 있어 암호화 통신에 대한 복호화 요구가 지속적으로 제기되고 있다. 이러한 웹서비스에서 HTTPS 암호화가 기본으로 권장되면서 웹방화벽은

* 명지전문대학 인터넷보안공학과 교수(제1저자)
** 덕성여자대학교 디지털소프트웨어공학부 교수
*** 한국예탁결제원 차장(교신저자)

웹서버에 설치되는 SSL/TLS 인증서를 이용하여 HTTPS 암호화 트래픽에 대한 복호화를 통해 암호화 트래픽에 대한 가시성을 확보하고있다. 즉, 인증서를 활용한 복호화 방식으로 암호화 웹서비스 트래픽에 대한 전용 가시성 장비를 지속적으로 개발하거나, 기존 네트워크 보안장비에 SSL/TLS 인증서 복호화 기능을 추가하여 웹서비스에 대한 가시성을 확보하기 위해 노력하고 있다.

그러나 클라우드 서비스가 <표 1>과 같이 급속하게 성장함에 따라[3] 기존 온프레미스 환경과 클라우드 서비스 환경이 상이하므로 클라우드 서비스 환경에서 보안 관리[4]를 위한 가시성의 확보가 중요한 이슈가 되고 있다.

<표 1> 전 세계 퍼블릭 클라우드 서비스 최종 사용자 지출 전망

서비스명	2021년	2022년	2023년
PaaS	86,943	109,623	136,404
SaaS	152,184	176,622	208,080
IaaS	91,642	119,717	156,276
총계	410,915	494,654	599,840

특히 정부가 추진하는 행정·공공기관 정보자원 클라우드 전환·통합 추진계획[5]에 따라 2025년까지 행정·공공기관 클라우드 전환을 위한 작업을 수행중에 있다. 이에 따라 클라우드 서비스 활용이 더욱 활성화 될 것으로 예상되며, 안전한 보안관제 서비스를 제공하기 위해서는 가시성 확보가 중요하다고 할 수 있다. 따라서 본 논문에서는 클라우드 환경에서 가시성 제공을 위한 연구를 수행하였으며, 2장에서는 클라우드 서비스의 개념 및 주요 유형에 대해서 설명하고, 3장에서는 클라우드 환경에서 가시성 제공 방안에 대해 설명하다. 4장에서는 제안한 방법들에 대해서 비교분석을 수행하고, 마지막으로 5장에서는 본 연구의 결론으로 구성하였다.

II. 클라우드 서비스의 개념 및 주요 유형

2.1 클라우드 서비스 개념

클라우드 컴퓨팅이란 서버, 스토리지, 네트워크, 어플리케이션 프로그램과 같은 각종 하드웨어 및 소프트웨어 등의 IT 자원을 이용자가 직접 설치하여 사용하는 방식이 아니라, 전기나 수도처럼 인프라 사업자가 가상의 네트워크 공간에 IT 자원을 구축해 놓고 이용자에게 신축적으로 제공하는 온-디맨드 방식의 서비스 체계를 말한다[6]. 따라서 이용자는 값비싼 IT 자원을 직접 구매하거나 소유할 필요 없이 자신이 필요할 때, 원하는 장소에서 필요한 만큼 자유롭게 빌려 쓰고 사용한 만큼만 비용을 지불하면 된다. 클라우드 컴퓨팅의 주요 특징은 다음과 같다[7].

① 온-디멘드 셀프 서비스(On-demand self-service): 인프라 사업자의 도움 없이 이용자가 원하는 서비스를 직접 선택하면 자동으로 제공

② 폭넓은 네트워크 접근성(Broad network access): 널리 사용되는 표준 방식 인터페이스로 언제 어디서든 네트워크만 있으면 접근이 가능하며, 다양한 디바이스(스마트폰, 태블릿, 노트북, PC 등)에서 접속하여 사용 가능

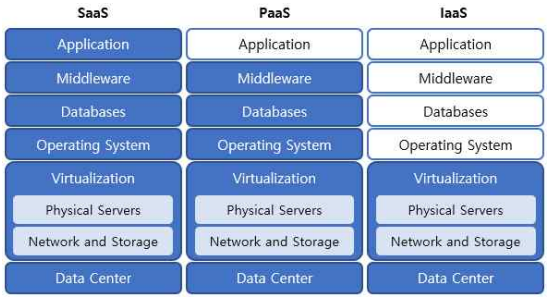
③ 자원 풀(Resource pool): 자원은 가상서버(컴퓨팅), 스토리지, 네트워크 대역폭 등을 포함하고, 컴퓨팅 자원은 다수의 사용자가 공유해야 하기 때문에 멀티테넌트(multi-tenant) 모델을 사용하며, 이용자는 제공된 자원의 정확한 위치를 알거나 관리할 수 없음

④ 빠른 적응성(Rapid elasticity): 즉시 사용 및 바로 돌려줄 수 있는 가변성이 보장되며, 자원을 빠르게 증설 및 반납 가능

⑤ 측정되는 서비스(Measured service): 사용한 만큼 비용을 지불하며, 자원(또는 서비스) 사용량은 모니터링, 조절, 보고되고 제공자와 사용자에게 투명하게 제공

2.2 클라우드 서비스 주요 유형

클라우드 서비스 유형에는 대표적으로 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)가 있다[8].



<그림 1> 클라우드 책임 공유 모델

IaaS(Infrastructure as a Service)는 서버, 스토리지, 네트워크 등 인프라 자원을 제공하는 서비스를 말한다. 가장 일반적인 서비스 형태로 Amazon EC2(Elastic Compute Cloud), S3(Simple Storage Service) 등이 이에 해당한다. 클라우드 서비스 제공업체(CSP, Cloud Service Provider)는 데이터센터를 구축해 가상화된 하드웨어를 제공하며, 서버, 네트워크, 스토리지 등 하드웨어 자원을 서비스 형태로 임대·제공하는 방식이다.

PaaS(Platform as a Service)는 인프라 자원과 함께 애플리케이션을 개발·테스트·실행할 수 있는 플랫폼까지 제공하는 서비스를 말한다. 구글 앱엔진(AppEngine), 마이크로소프트 애저(Microsoft Azure) 등이 이에 해당한다. PaaS는 운영체제, 데이터베이스, 웹서버 등 이용자에게 필요한 서비스를 개발할 때 필요한 플랫폼을 제공하는 방식이다. 클라우드 서비스 제공사(CSP)는 운영체제, 데이터베이스 등을 제공하고, 이용자는 이를 이용하여 응용프로그램을 개발할 수 있다.

SaaS(Software as a Service)는 표준화된 애플리케이션 기능을 제공하는 서비스를 말한다. 구글 G메일, 구글 앱스(GoogleApps), 마이크로소프트 오피스 365(Office 365) 등이 이에 해당한다. 서비스 제공자가 모든 인프라와 소프트웨어 제품을 제공하며, 사용자는 클라우드에서 제공하는 소프트웨어(또는 서비스)를 구매해 단말에 직접 설치하는 것이 아니라 웹을 통해 임대·제공하는 방식이다.

클라우드 서비스 유형에 따라 클라우드 서비스 제공자와 이용자가 클라우드 영역별 보안의 책임을 분담하며 이를 클라우드 책임 공유 모델이라 한다. 책임 공유 모델의 보안 책임은 클라우드 서비스 제공업체, 서비스 구성 및 특성 등에 따라 달라질 수 있다[6].

2.3 클라우드 플랫폼 보안 서비스

클라우드 제공업체는 클라우드 서비스를 보호하기 위하여 기본적으로 IDS, IPS, 웹방화벽, DDoS 서비스를 무상 또는 유상 서비스로 제공하고 있으며, 그 내용은 다음과 같다.

① 모든 Linux, Windows 서버는 보안 강화를 위해 보안 설정(Security Hardening)이 기본적으로 적용(무상)
② 서비스 종류에 따라 물리 서버를 가상화 환경 없이 단독으로 제공(유상)
③ 사용자가 생성한 서버, Cloud DB, App Safer, Secure Zone Firewall에서 발생하는 로그를 수집(유상)

위의 기능 이외에도 Anti-Virus, WAF, Anti-DDoS, IPS 서비스는 고객 필요에 따라 부가서비스(유상)로 제공한다. 이처럼 클라우드 환경에서도 기존 온프레미스 환경과 거의 유사한 보안시스템을 구성할 수 있다. 다만 데이터와 서비스 시스템에 대한 고객사의

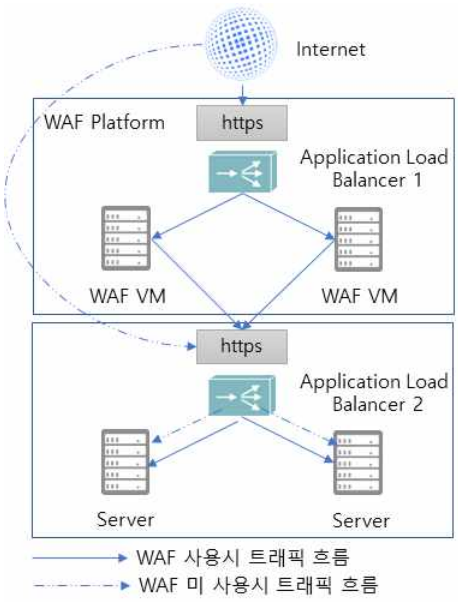
직접 통제가 온프레미스 환경보다 한계가 있어 클라우드 환경에서는 접근통제 역할이 더욱 강조되고 있다.

Ⅲ. 클라우드 서비스 환경에서 가시성 제공 방안

3장에서는 클라우드 서비스 환경에서 https로 전송되는 암호화된 패킷에 대해서 서비스를 이용하는 이용자 관점에서 가시성을 확보하는 방안에 대한 분석을 수행하였다.

3.1 로드밸런서를 활용한 가시성 확보

클라우드 서비스를 이용하는 이용자가 보안관제를 위한 가시성을 확보하기 위한 첫 번째 방안으로는 클라우드 사업자의 로드밸런서(기존의 L4 개념)에 웹서버 인증서를 설치하여 리버스 프록시로서 SSL/TLS 암호화 통신을 복호화하고 이후 평문 트래픽을 IDS, IPS와 같은 보안시스템에서 탐지룰에 대한 매칭을 하는 것이다. 구체적인 구성은 다음의 <그림 2>와 같다. 외부에서 유입되는 암호화 트래픽은 웹 방화벽이 있는 경우(WAF Platform), 애플리케이션 로드밸런서 1에서 복호화 된 후 평문으로 웹방화벽으로 전달되어 분석이 된다. 일반적으로 웹방화벽에 복호화 기능이 있어 성능 이슈가 발생하지 않는 경우 별도의 복호화 장비를 이용하지 않고 가시성을 확보할 수 있다. 만약 웹 방화벽(WAF Platform)이 없는 경우에는 인터넷에서 <그림 2>의 하단에 있는 애플리케이션 로드밸런서 2로 암호화된 패킷이 전달되어 복호화되며, 복호화된 평문 트래픽은 IPS 등 보안장비를 통해 웹서버에 전달된다.



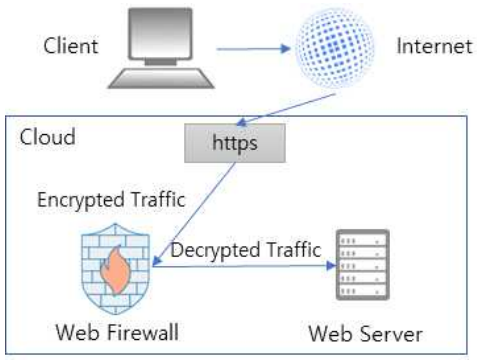
<그림 2> 로드밸런서를 이용한 SSL 복호화

3.2 보안 시스템을 활용한 가시성 확보

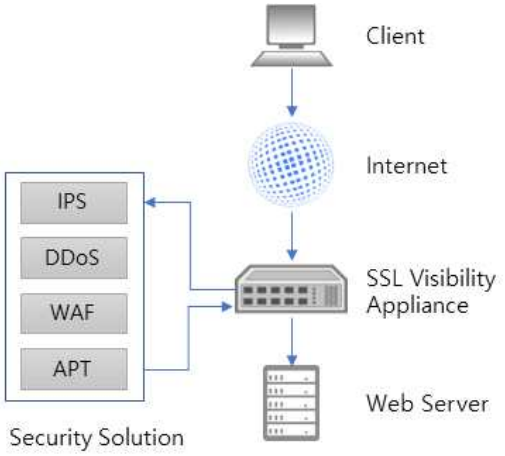
보안 시스템을 이용한 가시성 확보 방안은 클라우드 서비스 이용자가 클라우드 사업자 마켓에서 SSL/TLS 복화화 기능이 있는 웹 방화벽 등 보안시스템을 구매하여 리버스 프록시 기능을 사용하는 방안이다. 일반적으로 클라우드 사업자 마켓에서 구매할 수 있는 보안제품들은 모두 클라우드 워크로드에서 동작하는 SW 방식의 제품으로 구성되어 있으며, 클라우드 사업자의 기술 특성에 따라 보안시스템 제조사 지원 여부가 결정된다.

<그림 3>과 같이 보안시스템에서 SSL/TLS 암호화 통신을 복호화하고 평문을 전송하여 IDS/IPS에서 평문 트래픽을 수신하여 보안 룰 매칭을 수행하는 방식이다. 최근 출시되는 NIDS/NIPS는 리버스 프록시 기능이 가능하도록 SSL/TLS 복호화 기능이 있어 타 장비 없이도 단독으로 가시성 확보가 가능하다. 다만 복호화에 따른 성능 이슈가 발생할 수 있어 구축 전

사전 검토를 수행하는 것이 필요하다.



<그림 3> 보안시스템을 이용한 SSL 복호화



<그림 4> 전용장비를 이용한 SSL 복호화

3.3 SSL/TLS 복호화 전용장비 활용

AWS 등 일부 클라우드 마켓에는 SSL 가시성 전용 장비가 판매되고 있다. 이 방식은 <그림 4>와 같이 전용장비를 이용하는 방법으로 앞에서 설명한 로드 밸런서나 보안시스템을 이용한 구축 방법에 비해 성능 이슈로부터 자유롭다는 장점이 있으며, 서비스 안정성이 강조되는 구간에 주로 설치가 된다. 그러나 비용적인 측면에서 클라우드 사업자의 로드밸런서 또는 웹방화벽/IPS 부가기능을 활용한 방법에 비하여 부담이 된다. 이 방법은 SSL/TLS 암호화 패킷이 인터넷을 통해 SSL 가시성 장비에 도달하면 해당 패킷이 복호화되어 보안관제를 위해 IPS 등 보안 시스템에 전달되어 탐지룰에 대한 매칭을 수행한다. 검사를 수행한 패킷들은 다시 암호화되어 웹서버에 전달된다.

Ⅳ. 성능 비교 분석

3장에서 제안한 클라우드 서비스 환경에서의 가시성 제공 방안의 성능을 비교하기 위해서 [9]에서 사용된 성능 인자 값을 참조하여 비교분석을 수행하였다.

첫 번째 성능지표는 기밀성으로 크게 세 가지 유형으로 나누어 볼 수 있다.

- Full Reveal: 클라우드 서비스 내에서 데이터가 복호화된 상태로 이동하며, 중요정보의 유출 또는 변조 등에 취약할 수 있다.
- Partial Reveal: 클라우드 서비스 영역내에서 일부 구간에서는 복호화된 패킷 형태로 데이터가 전송되며, 일부 중요정보의 유출 또는 변조 등에 취약할 수 있다.
- Hidden: 클라우드 서비스 영역내의 모든 구간에서 암호화된 패킷 형태로 데이터가 전송되며, 중요정보의 유출 또는 변조 등의 공격을 차단할 수 있다.

두 번째 성능지표로는 기능성으로 보안 시스템의 운용 가능성을 의미한다. 이는 성능 이슈로도 볼 수 있으며, 본래 시스템의 기본 기능이외에 SSL/TLS 암호화 패킷의 복호화 작업에 따른 과부하로 인해 보안 기능의 수행과 관련되 지표이다.

- Full functionality: 다양한 보안시스템을 활용하여 탐지룰 매칭 등 모든 보안 검사 및 관리활동을 수행할 수 있다.
- Partial functionality: 보안관제를 수행하기 위한 보안기능의 일부 기능만 수행할 수 있다.

세 번째 지표로는 안전한 보안 서비스 제공을 위한 시스템 구축 비용을 들 수 있다. 클라우드 서비스의 보안관제 수행을 위한 구축비용도 실제 시스템 구축 시 중요한 요소로 작용하게 된다.

<표 2> 가시성 장비 구축방식에 따른 성능 비교 분석

Factor	로드밸런서 복호화	보안시스템 복호화	전용장비 복호화
Confidentialty	Full Reveal	Partial Reveal	Hidden
Functionality	Partial functionality	Partial functionality	Full functionality
Costs	Low	Low	High

로드밸런서를 활용한 가시성 확보의 경우에는 로드밸런서에서 SSL/TLS 암호화 패킷이 복호화되므로 클라우드 영역내에서는 기밀성 보장이 어려워 정보 유출의 이슈를 가지고 있다. 기능성 측면에서는 모든 데이터가 복호화되므로 보안시스템을 이용하여 공격탐지가 용이한 반면, 로드밸랜서에서 기본적인 패킷의 분배기능 이외에 암호화된 패킷의 복호화도 수행해야 되므로 성능 이슈가 있을 수 있다. 다만, 기존의 장비를 활용하여 SSL/TLS 암호화 패킷을 복호화하므로 구축비용이 상대적으로 저렴하다.

보안 시스템을 활용한 가시성 확보의 경우에는 보안시스템에서 SSL/TLS 암호화 패킷이 복호화되므로 클라우드 영역 안에서 보안시스템 이후에는 평문으로 전송되므로 일부 기밀성 보장이 어렵다고 볼 수 있다. 기능성 측면에서는 보안시스템에서 데이터가 복호화되므로 공격탐지가 용이한 반면, 보안시스템의 기본적인 보안 관리 기능 이외에 암호화된 패킷의 복호화도 수행해야 되므로 성능 이슈가 발생할 수 있다. 구축비용의 경우 기존 장비를 활용하므로 상대적으로 저렴하다고 볼 수 있다.

SSL/TLS 복호화 전용장비 활용의 경우에는 가시성 장비에서 암호화된 패킷을 복호화하여 보안시스템에 전달하고, 다시 이 패킷을 재암호화를 수행한 후 웹서버로 전달하므로 데이터의 기밀성을 유지할 수 있다. 기능성 측면에서도 가시성 전용장비를 활용하므로 보안시스템에서 공격탐지가 용이하고, 성능 이슈가 발생하지 않는다. 다만, 가시성 전용장비 구축에 따른 추가적인 비용이 발생하게 된다.

따라서 클라우드 서비스 보안관제 시스템을 자체적으로 구축하기 위해서는 기밀성, 기능성(성능), 구축 비용과 서비스 중요도를 고려하여 구축 방법을 선택해야 된다. 특히 보안적인 측면에서는 로드밸런서나 보안시스템을 이용한 구축 방법의 경우, SSL 암호화 통신의 복호화 이후부터 웹서버까지 평문 통신을 하게 된다. 이러한 경우 정보 유출의 이슈를 고려하여 구축하여야 하며, SSL/TLS 복호화 전용장비를 사용할 경우 가시성 장비에서 재암호화 후 웹서버로 전달하여 데이터의 기밀성을 유지할 수 있다는 이점을 가지고 있다.

Ⅴ. 결론

정부가 추진하는 행정·공공기관 정보자원 클라우드 전환·통합 추진계획에 따라 2025년까지 행정·공공기관 클라우드 전환을 위한 작업을 수행중에 있다. 또한 민간에서는 이미 금융을 포함하여 많은 분야의 회사들이 클라우드 서비스를 이용하고 있으며, 그 사용량은 점점 더 확대될 것으로 예상된다. 이에 따라 기존 온프레미스 환경에서 주로 사용하던 방식인 침입탐지 혹은 침입방지시스템 등 정보보호시스템을

구축하고, 탐지룰을 설정하여 다양한 해킹공격 방지 및 로그 분석을 통한 이상행위를 탐지하던 방식이 Iaas, PaaS, SaaS 등 클라우드 서비스 유형에 따라 더 이상 유효하지 않게 변경되었으며, 이에 따라 클라우드 서비스 환경에서 가시성 확보가 중요한 이슈가 되었다.

본 논문에서는 클라우드 서비스 환경에서 가시성을 제공할 수 있는 방안에 대한 분석을 수행하였다. 클라우드 서비스 환경에서 가시성을 제공하는 방안으로는 로드밸런서를 활용하는 방법, 보안 시스템을 활용하는 방법, SSL/TLS 복호화 전용장비를 활용하는 방법들이 있으며, 이러한 방법들에 대해서 기밀성, 기능성(성능), 구축비용 측면에서 성능비교를 수행하였다. 이를 통해 각 가시성제공 방안들에 대해 장단점을 제시하였으며, 최근 침해사고 사례와 가시성 장비의 시장 동향을 볼 때, 클라우드 관제 환경 구축시 반드시 암호화 트래픽에 대한 가시성을 확보하는 것이 요구된다.

향후 연구계획으로는 요즘 이슈가 되고 있는 제로트러스트 기술을 클라우스 서비스 환경에서 제공할 수 있도록 하는 가시성 제공방안에 관한 연구를 수행할 예정이다. 이를 통해 클라우드 서비스를 이용할 때 좀 더 안전한 서비스 환경을 제공할 수 있을 것이라 예상된다.

참고문헌

[1] 김태경, “HTTPS 웹 사이트 차단의 익명성 제공 방안 연구,” 디지털산업정보학회논문지, 제15권, 제1호, 2019년, pp.53-59.

[2] Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V., "Decrypting SSL/TLS traffic for hidden threats detection," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp.143-146.

[3] 가트너, 전 세계 퍼블릭 클라우드 서비스 최종 사용자 지출 전망, 2022년 10월, (https://www.itworld.co.kr/numbers/82001/262438, Access: 2023년 1월 26일)

[4] Singh, Ashish, and Kakali Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, Vol. 79, 2017, pp.88-115.

[5] 행정안전부, 행정·공공기관 정보자원 클라우드 전환·통합 추진계획, 2021년 7월, (https://www.korea.kr/common/download.do?fileId=195380178&tblKey=GMN, Access: 2023년 1월 26일)

[6] 한국지능정보사회진흥원, 클라우드의 미래보습과 보안, 미래2030 제2권, 2020년 12월.

[7] 이정림·장항배, “클라우드컴퓨팅 시스템 환경의 효과적 위험분석평가 방법에 관한 연구,” Journal of Platform Technology, 제9권, 제2호, 2021년, pp.10-25.

[8] 오광진·정기문·조혜영·박준영·박경석, 초고성능컴퓨팅인프라 클라우드 서비스 구축을 위한 제언, KISTI ISSUE BRIEF, 제46호, 2022년 8월.

[9] Poh, G. S., Divakaran, D. M., Lim, H. W., Ning, J., & Desai, A., “A survey of privacy-preserving techniques for encrypted traffic inspection over network middleboxes,” arXiv preprint arXiv:2101.04338, 2021.

■ 저자소개 ■

김 태 경
Kim Taekyung

2017년 9월~현재
명지전문대학 교수
2008년 3월~2017년 8월
서울신학대학교 교수
2006년 3월~2008년 2월
서일대학교 교수
2005년 8월 성균관대학교
전기전자및컴퓨터공학과(공학박사)

관심분야 : 네트워크보안, IoT 보안,
개인정보보호
E-mail : tkkim@mjc.ac.kr

백 남 균
Baik Namkyun

2023년 3월~현재
덕성여자대학교 교수
2019년 3월~2023년 2월
부산외국어대학교 교수
2000년~2017년
한국인터넷진흥원 수석연구원
2011년 2월 숭실대학교 전자공학과(공학박사)

관심분야 : 스마트융합보안, 정보보안컨설팅
E-mail : white-knight@daum.net

김 정 협
Kim Junghyup

2011년 11월 ~ 현재
한국예탁결제원 차장
2001년 7월 ~ 2011년 11월
한국인터넷진흥원 책임연구원
1998년 2월 고려대학교 응용전자공학과
(공학석사)

관심분야 : 네트워크보안, 디지털포렌식,
보안정책
E-mail : hyup92@hotmail.com

논문접수일 : 2023년 1월 28일
수정접수일 : 2023년 2월 13일
게재확정일 : 2023년 2월 14일