Journal of Korea Multimedia Society Vol. 20, No. 1, January 2017(pp. 58-65)
https://doi.org/10.9717/kmms.2017.20.1.058

클라우드 기반 협업 콘텐츠 프랙탈 서비스 및 침입탐지 프레임워크

박상현[†], 이혜주[††], 이석환[†††], 권기룡[††††], 박윤경[†††††], 문경덕[††††††]

Collaboration Contents Fractal Service and Intrusion Detection framework based on Cloud

SangHyun Park[†], Hyejoo Lee[††], Suk-Hwan Lee[†††], Ki-Ryong Kwon[††††], Yun Kyoung Park[†††††], Kyoung Deok Moon[††††††]

ABSTRACT

The recent years, the cloud-based paradigm of cloud services are developed rapidly, it come with many a new problems. However, the collaboration between a individual with other users is still difficult. Cloud service is considered when users need to take advantage of security and the availability of cloud services. In this paper, we proposed an detection framework to detect an intrusion attack that threaten to cloud-based collaboration services and cloud security. Identify vulnerabilities and prepare for the safety of the collaboration services to create a variety of content in the cloud, it help to prevent the threats.

Key words: Cloud Service, Collaboration Contents, Intrusion Detection Framework

1. 서 론

최근 5년 전까지 컴퓨터를 사용하는 이용자들은 자신의 작업한 서류, 신상정보와 같은 데이터를 저장하거나 다른 이용자에게 전송하기 위해 USB또는 CD를 사용하여 자신의 데이터를 다른 사용자에게 전달하는 방식을 이용해왔다. 하지만 급속한 컴퓨팅 기술과 인터넷 발달로 USB나 CD로 물리적인 매체를 이용하여 데이터를 전송하는 방식이 아닌 인터넷으로 e메일이나 웹 서버에 저장하여 다른 사용자들과 데이터를 공유하거나 전송할 수 있는 방식을 이용하고 있다. 이러한 웹 서버 서비스 중에 클라우드 서비스는 사진이나 문서, 동영상 등 각종 콘텐츠를 클라우드 서버에 저장한 뒤 인터넷으로 접속해 노트북이나 스마트폰 등 다양한 기기로 이용할 수 있는 서비스이다.

※ Corresponding Author : Ki-Ryong Kwon, Address: (608-737) 45 Yongso-ro, Namgu, Busan, Korea, TEL : +82-51-629-6257, FAX : +82-51-629-6230, E-mail : krkwon@pknu.ac.kr
Receipt date : Dec. 28, 2016, Approval date : Jan. 6, 2017
[†] Dept. of IT Convergence and Application Engineering, Pukyong Nat'l University
(E-mail : hicaru_sai@naver.com)
[††] Dept. of IT Convergence and Application Engineering, Pukyong Nat'l University
(E-mail : Hyejoo2010@gmail.com)
[†††] Dept. of Information Security, TongMyong University
(E-mail : sklee@tu.ac.kr)
[††††] Dept. of IT Convergence and Application Engineering, Pukyong Nat'l University
(E-mail : krkwon@pknu.ac.kr
[†††††] Wearable Computing Research Team, ETRI
(E-mail : parkyk@etri.re.kr)
[††††††] Wearable Computing Research Team, ETRI
(E-mail : kdmoon@etri.re.kr)
※ This work was supported by the ICT R&D program of MSIP/IITP. [R0126-16-1112, Development of Media Application framework based on Multi-modality which enables Personal Media Reconstruction and the Technological Innovation R&D Program (C0407372) funded by the Small and Medium Business Administration (SMBA, Korea)".

클라우드 서비스 패러다임의 급속히 변화하는 서비스 중에 클라우드 서버에 저장되어있는 데이터들을 한 이용자가 아닌 여러 이용자들이 한 데이터를 이용자들끼리 정한 콘텐츠에 맞도록 서로의 의견을 제시하며 수정하는 클라우드 기반의 협업이 새로운 이슈로 떠오르고 있다[1]. 이러한 협업이 가능한 클라우드 서비스는 일반적인 클라우드 서비스보다 더 다양한 콘텐츠를 제작할 수 있다. 예를 들어, 영상물 제작, 시나리오 제작, 업무와 관련된 작업 등 사용자 개인 혼자서 제작하기 어려운 콘텐츠를 협업을 통하여 개인이 아닌 여러 사용자들과 함께 협력하여 보다 쉽고, 완성도가 더 높은 콘텐츠를 제작할 수 있는 협업 서비스를 통하여 콘텐츠를 제작할 수 있다[2]. 클라우드 서비스는 아웃소싱 서비스이기 때문에 외부의 침입으로부터 완전하게 안전하지 못하기 때문에 사용자에 대한 보안과 가용성은 클라우드 서비스를 이용, 유지하기 위해 고심해야할 가장 중요한 부분 중 하나이다[3]. 특히 DDos 공격과 같은 클라우드 서비스의 가용성을 저하시키는 공격은 클라우드 서비스의 신뢰성을 저하시키는 위협이 될 수 있다.

본 논문에서는 클라우드 기반 협업 콘텐츠의 프랙탈 서비스 및 침입탐지 프레임워크를 제안한다. 제안한 방법은 프랙탈 서비스를 포함한 클라우드 기반 협업 콘텐츠 서비스들의 보안 및 가용성에 대하여 침입탐지 프레임워크를 제안함으로써 공격자의 DDos 공격에 대비하여 침입하거나 침입하기 전에 미리 감지하여 클라우드 기반 협업 서비스의 보안에 대한 취약점을 보완하는 것을 제안한다. 기존의 방법에서는 공격이 발생한 이후에 보안이 작동하기 때문에 공격을 방어한다고 하더라도 전체 트래픽의 2~5%의 일정 피해를 입게 된다. 하지만 제안 기법은 공격이 발생하기 전에 사전에 미리 감지하여 보안이 되므로 트래픽 피해가 존재하지 않는다.

본 논문의 구성은 다음과 같다. 우선, 2장에서는 클라우드 기반 협업 서비스 소개를 기술한다. 그리고 3장에서는 클라우드 서비스를 위협하는 DDos 공격 종류와 효과에 대해 알아본다. 4장에서는 클라우드 기반 협업 침입탐지 프레임워크 요구사항에 대해 정리하고, 5장에서는 클라우드 기반 협업 침입탐지 프레임워크를 분석한다. 6장에서는 클라우드 기반 협업 콘텐츠 서비스에서 침입탐지 프레임워크의 기대효과와 향후 연구 내용에 대해 기술한다.

2. 클라우드 기반 협업 콘텐츠 서비스

클라우드 기반 협업 콘텐츠 서비스(Cloud-based Collaboration Contents Service)는 웹기반 애플리케이션을 활용하여 대용량의 데이터베이스를 인터넷 가상공간에서 정보를 입력, 저장, 가공할 수 있게 하는 환경에서 사용자들 간의 협업을 통하여 의견제시 및 질의문답, 역할분담 등과 같은 협업을 통한 서비스를 말한다[4].

이러한 클라우드 기반 협업 서비스를 보여주는 프랙탈(Fractal) 콘텐츠 프로토타입이 있다. 이 프로토타입은 UTS-알파라 불리는 공동 제약 연구 프로젝트를 지원하는 콘텐츠 공간을 중심으로 하는 프로토타입이며, 문서 라이브러리에서 콘텐츠를 부가하여 회원들간의 부가된 콘텐츠에 대해 데이터를 올리는 프로토타입이다. 프랙탈 프로토타입에서는 콘텐츠 공간, 활성동작, 다른 사용자의 확장 등 3가지의 기능들을 가진다.

1) 콘텐츠 공간: 다양한 콘텐츠, 협업 도구, 사용자 정의 활성 행동과 함께 가지고 있는 호스팅 작업을 하는 공간이다.

2) 활성 동작: 콘텐츠, 메타데이터, 자동화 처리 서비스, 다른 사용자들에 의해 작업에 관련된 콘텐츠 공간 내에서 동작하는 기능을 확장을 정의하기 위한 동작이다. 필요에 따라 수동으로 호출할 수 있거나, 콘텐츠 공간 또는 시간에 의해 자동으로 호출할 수 있다. 호출은 하나의 콘텐츠 객체 또는 여러 객체를 포함할 수 있다. 수정과 같은 문서의 최신 PDF 버전 생성으로부터 복잡성의 범위는 하나의 문서에 여러 협업 과정에서 정보를 자동으로 대조한 작업흐름을 실행한다.

3) 다른 사용자의 확장: 마켓 플랫폼에서 사용자가 플랫폼을 통해 구입할 수 있게 사용자 정의하고, 확장을 통하여 다른 사용자를 활성화하여 마켓 플랫폼을 다른 사용자도 이용 가능하도록 오픈API를 제공한다.

2.1 프랙탈 프로토타입 개요

프랙탈 프로토타입은 UTS-알파라 불리는 공동 제약 연구 프로젝트를 지원하는 콘텐츠 공간을 중심으로 연구되고 있다.

Fig. 1에서는 보고서 콘텐츠를 생성하는데 UTS-

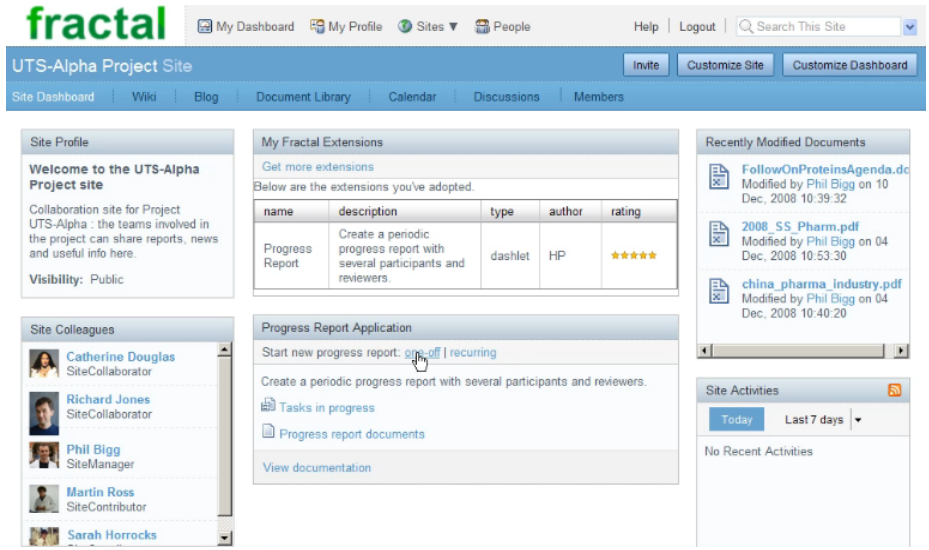

Fig. 1. Collaboration contents of FRACTAL prototype.

Alpha 콘텐츠 공간에 기능을 추가할 수 있도록 콘텐츠 공간을 확장하여 생성한다. 사용자가 필요한 기능을 찾을 수 있도록 검색과 찾아보기와 같은 기능들을 제공하고 있다. 여기서 확장은 문서 라이브러리에 보고서를 작성하는데 필요한 단계를 조율하는 iBPM을 워크플로우에 추가했다. 목표와 명령을 달성하기 위해 실행되어야 할 스텝들을 플로우차트를 이용하여 표현함으로써 콘텐츠 목표를 형성화하고 있다[5].

프랙탈 프로토타입은 최종 사용자가 자신의 구상한 콘텐츠의 특성을 작동하는 시스템을 성공적으로 사용하지만, 다른 주요 ECM 플랫폼이 아닌 프로토타입을 구축하는 것은 멀티-테넌트, 클라우드 규모의 협업 플랫폼의 기술적인 부분이 필요로 한다[5].

2.2 프랙탈 프로토타입의 기술

프랙탈 프로토타입이 필요로 하는 기술로는 대표적으로 멀티 테넌트 기술을 볼 수 있다. 멀티 테넌트 기술은 대부분의 클라우드 기반 서비스는 본질적으로 멀티 테넌트이며, 이런 방식은 프랙탈 프로토타입 규모에서 서비스를 실행하는데 필요한 규모를 처리하는 가장 효율적인 방법이다.

일반적으로 멀티 테넌트 소프트웨어의 정의는 실제 서비스가 하나 또는 다수의 사용자간의 큰 인스턴스를 나누는 동안, 소프트웨어의 사용자들 자신의 인스턴스를 부여하는 것을 말한다. 사용자 데이터의 분리는 개인이 자신의 데이터를 공유할 수 있는 것을 불가능하도록 만든다. 하지만 멀티 테넌트 협업 서비스를 통해 사용자들간의 관련 콘텐츠, 프랙탈 프로토타입의 콘텐츠에서 협업 활동을 사용할 수 있다[6].

3. 클라우드 기반 협업 DDos 공격위협

클라우드 컴퓨팅 환경에서 DDos 위협은 외부 공격과 내부 공격, 이 2가지로 크게 분류할 수 있다. 외부 공격은 좀비 PC 또는 좀비 클라우드로부터의 DDos공격이 가능하며, 내부 공격은 VM(Virtual Machine)간의 DDos공격, VM으로부터의 Hypervisor 공격, 클라우드 서버를 이용한 DRDoS (Distributed Reflection Denial of Service) 공격으로 분류한다[7]. 서비스 시나리오는 Fig. 2와 같이 User, Access Control, Virtual Machine, Contents로 클라우드 컴퓨팅 모델 시나리오를 구성하였다[7].

3.1 외부 공격

Fig. 3에서 좀비 PC/ 좀비 클라우드의 DDos 공격은 분산 처리 용량을 초과하는 대용량 트래픽 공격이 가능하다. 수십, 수백만대의 좀비 PC를 생산하여 DDos 공격을 하거나 대규모의 좀비 클라우드의 가상머신을 이용한 DDos 공격을 하는 경우가 발생하며, 좀비 PC와 좀비 클라우드가 동시에 공격하는 경우에는 대

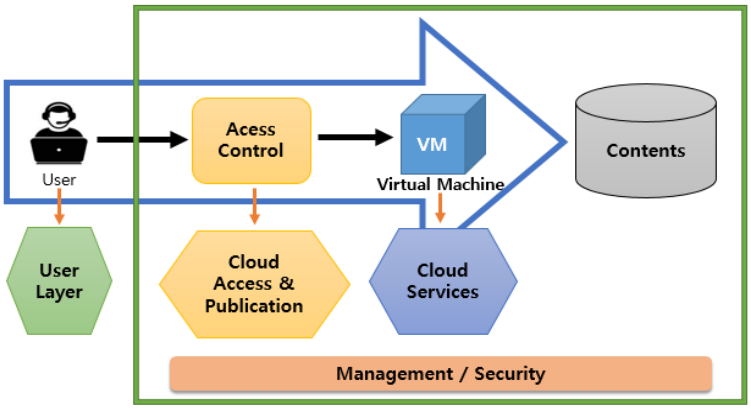

Fig. 2. Cloud Computing Model Service Scenario.

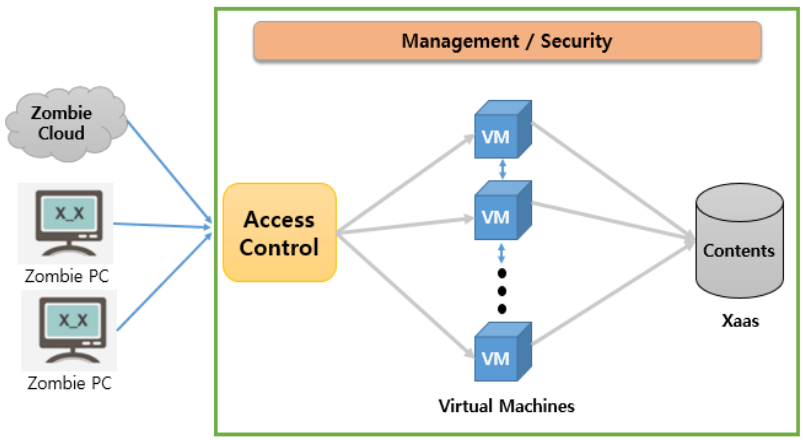

Fig. 3. DDos attack of Zombie PC/Zombie cloud.

형 클라우드 서비스 제공자에게도 큰 위협이 된다.

3.2 내부 공격

Fig. 4에서 클라우드 서버의 일부 VM을 좀비로 감염시켜 특정 사용자의 VM를 공격하여 피해주는 DDos 공격 방법이 있다. 공격받아 손상된 VM는 좀비에 감염되어 또 다시 다른 특정 사용자의 VM을 공격하는 좀비 VM으로 변질 될 수 있다.

또 다른 내부 공격으로는 클라우드의 감염된 VM들을 장악하여 Hypervisor를 DDos 공격하는 경우가 있다. 공격받은 Hypervisor가 상태 불능이 되거나 권한을 강탈하여 클라우드 내의 서비스 및 유저들의 데이터를 유출 또는 임의로 변경하여 유저들과 제공자에게 막대한 피해를 줄 수 있다. 감염된 VM들이 Hypervisor를 DDos 공격하는 과정은 Fig. 5에서 설명하고 있다.

마지막으로 클라우드 서버를 이용한 DRDos 공격이 있다. Fig. 6에서 보여주듯이 클라우드 서버의 일

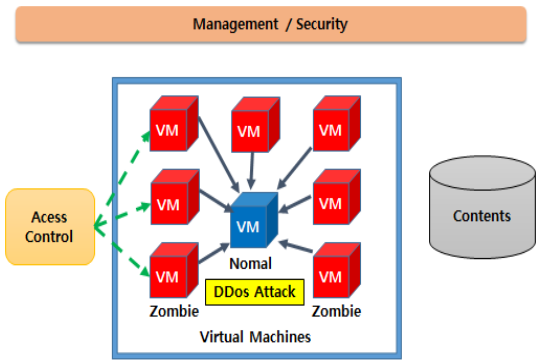

Fig. 4. DDos attacks between VMs.

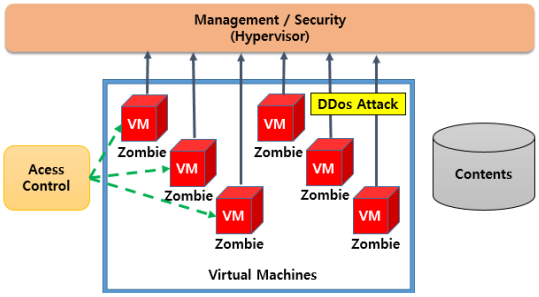

Fig. 5. Hypervisor attack from VMs.

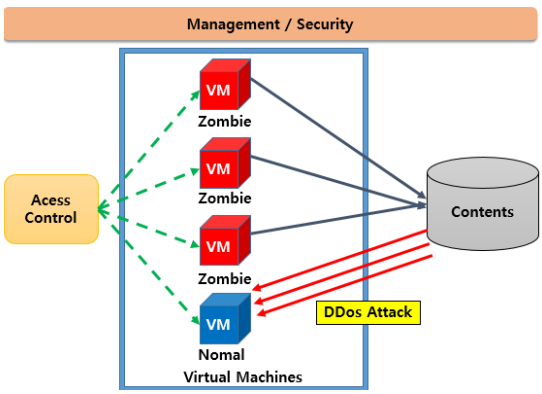

Fig. 6. DRDos attacks using cloud server.

부 VM에서 IP를 공격대상의 IP주소로 위조하여 클라우드 서버에 서비스 요구를 하면 클라우드 서버에서는 서비스 요구에 대한 응답을 한다. 하지만 공격 대상인 VM은 서비스 요구를 하지 않았기 때문에 클라우드 서버의 응답을 받지 않는다. 그렇게 되면 클라우드 서버에서는 응답메시지가 전달하는 과정에서 분실되거나 메시지가 변조되어 훼손되었다고 오해하게 된다. 그래서 클라우드 서버에서는 보통 3차례의 응답메시지를 다시 공격 대상 VM에게 보내게 된다. 이런 경우, 좀비 VM의 수가 적더라도 좀비 PC 수의 3배 이상의 DDos 공격 효과를 보게 된다.

4. 클라우드 기반 협업 침입탐지 프레임워크 요구사항

클라우드 기반 협업 침입탐지 프레임워크의 요구사항으로는 인프라 공격에 대한 정확하고 즉각적인 경보, 침입탐지 시스템 환경의 전송 데이터 보안 및 무결성 보장, 클라우드 협업 서비스 환경이 고려된 사용자 인터페이스, 침입탐지 프레임워크 구조의 확장성과 유연성 확보, 가상 머신 성능 보장, 안전한 데이터 통신을 위한 인증 및 암호화 등 6가지의 요구사항으로 정리하였다[8,9].

1) 인프라 공격에 대한 정확하고 즉각적인 경보: 공격자는 높은 효과를 얻기 위한 다단계 공격을 전개하지만 각 단계마다 공격을 보고하고 그 연관성을 판단할 수 없기 때문에 분산 서비스 거부 또는 웜 바이러스와 같은 공격들의 탐지가 어렵다. 클라우드 환경의 침입탐지 시스템은 동일한 상황 또는 긍정오류 경보를 줄이고 다단계 공격을 정확하게 감지할 수 있는 메커니즘이 포함되어야 한다.

2) 침입탐지 시스템 환경의 전송 데이터 보안 및 무결성 보장: 호스트 아이피 주소, 포트, 서비스 모델, 사용자의 가상호스트 위치, 침입탐지 시스템에서 다른 침입탐지 시스템으로의 데이터 이동 등의 중요한 정보가 공격자의 표적이 될 수 있다. 암호화 데이터, 개인 커뮤니케이션 채널 사용 등의 해결방안을 제공해야 한다.

3) 클라우드 협업 서비스 환경이 고려된 사용자 인터페이스: 사용자는 자신의 가상화된 자원에 대하여 다양한 탐지 방법, 규칙 설정 및 특정 탐지 방법에 대한 임계값을 제어할 수 있어야 한다. 그러나 클라우드 기반 협업 환경에서는 다수의 클라우드 제공자에 의해 서비스가 제공되므로 이러한 환경이 고려되어 침입 탐지 시스템에 대한 설정이 가능해야 한다. 클라우드 환경의 특성상 다수의 가상 머신과 침입탐지 기능으로 인해 그 설정이 복잡해 질 수 있으므로 사용자 설정 기능의 단순화와 투명성이 제공되어야 한다.

4) 침입탐지 프레임워크 구조의 확장성과 유연성 확보: 협업 클라우드 환경에서 가상 머신은 사용자의 요구에 따라 자원을 할당, 회수, 이동이 빈번하게 이루어진다. 따라서 이러한 변화에 즉 각적인 프레임워크 구조 확장성과 유연성이 보장되어야 한다.

5) 가상 머신 성능 보장: 협업 클라우드 환경에서는 다수의 가상머신 간의 협업 침입탐지를 위해서 대규모의 데이터 수집 및 분석이 필요하지만 침입탐지 프로세스로 인한 가상머신의 성능 저하를 초래하기 때문에 침입탐지에 필요한 자원할당은 최소한으로 이루어져야 한다.

6) 안전한 데이터 통신을 위한 인증 및 암호화: 클라우드 컴퓨팅 환경에서는 침입탐지 시스템과 가상

머신이 같은 물리적인 공간에 존재할 수 있으며 또한 클라우드 서비스 이용자가 악의적인 목적으로 침입탐지 시스템의 정보를 유출 및 유실을 유도할 수 있다. 이는 침입탐지 시스템의 기능을 저하시키거나 마비시킬 우려가 높다. 따라서 정보 유출이 발생하더라도 일반 사용자가 이를 알지 못하도록 암호화가 요구되어야 한다.

5. 제안한 클라우드 기반 협업 침입탐지 프레임워크

위에서 언급한 클라우드 기반 협업 DDos 공격위협과 침입탐지에 대한 요구사항에 대하여 알아보았다. 클라우드 기반 협업 콘텐츠 서비스들은 공격자가 VM을 공격대상으로 삼거나 VM를 좀비VM으로 전염시켜 사용자들과 서비스 제공자에게 피해는 주는 DDos 공격에 취약하다는 점과 취약점을 보완하기 위해 필요한 요구사항들을 연구하여 클라우드 기반 협업 침입탐지 프레임워크를 제안하고자 한다. 제안된 기법은 침입탐지 요구사항을 준수하면서 클라우드 서비스의 DDos 공격을 사전에 미리 대비하여 침입을 막고자 하는 것을 목적으로 삼고 있다. Fig. 7는 클라우드 기반 협업 프랙탈 서비스 침입탐지 프레임워크를 설계하였다.

5.1 초급 탐지기

침입탐지 시스템은 각 가상 머신을 모니터링하기 위해 각 서버에 배치되고 각 호스트에서 작동한다. 초급 탐지기에서 경보 알림, 분석, 사용자 설정에서 각각의 역할을 부여한다. 경보 알림에서는 임계값을 기준으로 초과 시 초급 경고를 생성하고 종합적인 분석을 위해 암호화 후 침입탐지 송신기로 전송한다. 분석은 호스트의 잠재적인 침입을 탐지하기 위해 네트워크 트래픽, 메모리 시스템, 파일 시스템 등에 대한 데이터를 수집하고 분석한다. 사용자 설정에서는 침입탐지 관리자에서 설정한 사용자의 초급 탐지기 환경 설정 및 서비스 모델정보는 가상 머신의 초급 탐지기에 적용하기 위해 침입탐지 송신기로부터 정보를 제공받는다.

5.2 침입탐지 송신기

각 클라우드 지역의 독립적인 보안 노드의 구성요소이며 클라우드 사용자들의 로컬 가상 머신을 모니터링 하는 분산된 초급 탐지기 생성 및 관리를 담당한다. 또한 초급 탐지기에서 모인 초급 경보를 바탕으로 의심되는 신호는 하이퍼 경보로 침입탐지 관리자에게 전송하게 된다. 침입탐지 송신기에서도 침입탐지 생성기, 경보 연관기, 형식 변환기로 역할을 나누어 담당한다. 침입탐지 생성기는 가상 머신들을 모니터링 하는 초급 탐지기의 구성과 생성을 담당하고 침입탐지 관리자에게 통신을 담당하고 있다. 경보 연관기는 초급 탐지기에서 발생한 초급 경보와 침입탐지 관리자에서 제공하는 블랙리스트의 공격패턴을 연관지어 공격의도 여부를 판단하고 통계기반의 일정 값을 초과하는 경우 침입으로 인식하여 침입탐지 관리

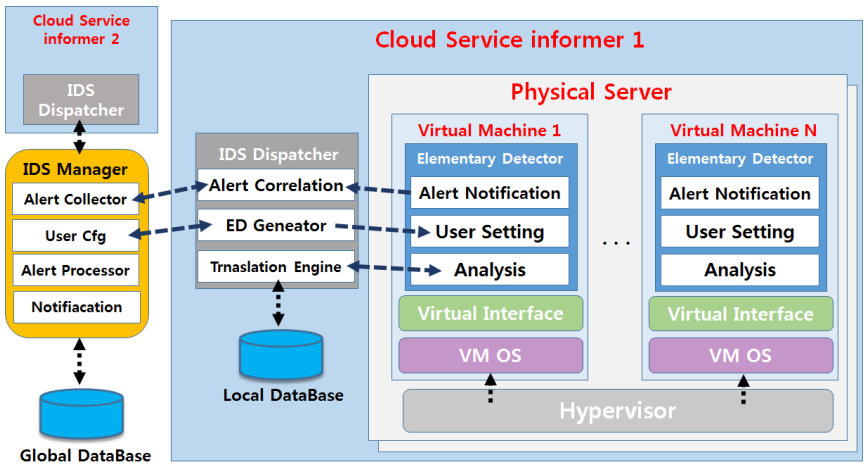

Fig. 7. Collaboration FRACTAL service intrusion detection framework based on cloud.

자와 클라우드 서비스 관리자에게 이를 알린다. 형식 변환기는 클라우드 영역에서 존재하는 모든 초급 탐지기에서 발생하는 모든 초급 경보들을 형식 변환기를 통해 로컬 데이터베이스에 저장되고, 저장된 경보들은 침입탐지 관리자에서 사용가능 하도록 공통 형식으로 변환시키는 역할을 한다.

5.3 침입탐지 관리자

침입탐지 프레임워크의 중앙 관리 컴포넌트로서, 클라우드 서비스 사용자와 초급 탐지기 사이에서 필요한 정보 전달의 역할을 수행한다. 침입탐지 관리자에서는 사용자 설정, 통지, 경보 수집기, 경보 처리기 크게 4가지 역할을 한다. 사용자 설정에서는 사용자의 침입탐지 시스템의 구성 정보를 수집하여 사용자의 가상머신에 초급 탐지기들을 생성하고 구성에 필요한 기능, 임계값 등을 설정할 수 있다. 통지에서는 서비스 관리자에게 할당된 자신의 자원에 침입이 있는 경우, 각 사용자들과 서비스 관리자에게 이를 통보하는 역할을 수행한다. 경보 수집기는 감지된 경보 메시지를 포함한 모든 메시지의 수신을 담당한다. 수집된 경보 메시지는 글로벌 데이터베이스에 저장되어 경보 처리에 의해 분석된다. 경보 처리기는 프레임워크의 최상위 모듈로 글로벌 데이터베이스에 저장된 초급 경보 및 하이퍼 경보를 분석하는 역할을 한다. 분석을 통해 침입공격 패턴 일치 여부를 판단하고 새로운 공격패턴은 블랙리스트에 추가하여 각 침입탐지 송신기인 로컬 데이터베이스로 전송한다.

6. 결 론

본 논문에서는 클라우드 기반 협업 콘텐츠 프랙탈 서비스 환경에서 침입탐지 프레임워크를 제시하였다. 침입탐지 공격 시나리오에서는 공격 대상이 VM이거나 VM을 전염시켜 다른 VM을 공격하거나 Hypervisor를 공격하여 사용자들과 서비스 제공자에게 피해를 준다. 기존의 방법에서는 공격이 발생한 이후에 보안이 작동하기 때문에 공격을 방어한다고 하더라도 전체 트래픽의 2~5%의 일정 피해를 입게 된다. 이러한 취약점을 보완하기 위해 침입공격에 대하여 VM의 트래픽 크기와 자원 사용률을 검사하는 모듈인 초급 탐지기, 침입탐지 송신기, 침입탐지 관리자를 추가하여 클라우드 환경에서 발생가능한 침입공격을 사전에 방지하도록 제안하였다. 이를 통해 클라우드에서 다양한 콘텐츠를 만드는데 필요한 협업 서비스의 보안에 대한 취약점을 미리 파악 및 대비하여 위협을 사전에 차단이 가능하다.

향후 연구에서는 침입탐지 프레임워크를 구현하여 협업 클라우드 환경에서 효율적인 침입탐지를 위한 알고리즘 및 분석 방법에 대흔 연구를 수행할 것이다.

REFERENCE

[1] E. Jetal, *Content-Centered Collaboration Spaces in the Cloud*, HPL Tech Report HPL-2009-11. Institute of Electrical and Electronics Engineers Internet Computing special issue on Cloud Computing, Jan. 2009.

[2] H.J. Lee, K.R. Kwon, S.H. Lee, Y.K. Park, and K.D. Moon, “Design of Open Scenario Structure for Content Creation Service Based on User Defined Story,” *Journal of Korea Multimedia Society*, Vol. 19, No. 2, pp. 170-179, Feb. 2016.

[3] ZDNet, http://www.zdnet.com/article/firms-headed-for-cloud-security-wake-up-call/, (accessed June 20, 2016).

[4] D. Banks, J.S. Erickson, and M. Rhodes “Toward Cloud-based Collaboration Services,” *HotCloud,* June 2016.

[5] Fractal Conceptual Prototype Videos, http://www.hpl.hp.com/breweb/hp-fractal-prototype/, (accessed June 14, 2016).

[6] Alfresco Share, http://tinyurl.com/3z7wkh, (accessed June 14, 2016).

[7] J.Y. Park, S.H. Na, and E.N. Huh, “An Analysis on the DDos Threats to Cloud Computing,” *Proceedings of Symposium of the Korean Institute of Communications and Information Sciences*, pp. 314-315, June 2011.

[8] J.Y. Park, S.H Na, and E.N Huh, “Personal Cloud Computing Security Framework,” *Proceeding of Institute of Electrical and Electronics Engineers Asia-Pacific Services Computing Conference*, pp. 671-675, Nov.

2010.
[9] D.A. Adjeroh, M. Ryynanen, and K.C. Nwosu, "Multimedia Database Management Issues," *Journal of Korea Multimedia Society*, Vol. 4, No. 3, pp. 24-33, March 1997.

박 상 현

2015년 동명대학교 컴퓨터공학과 학사 졸업
2015년~현재 부경대학교 IT융합응용공학과 석사 재학중
관심분야 : 클라우드 컴퓨팅, 영상처리

이 혜 주

1990년 부경대학교 전자계산학과 (학사)
1997년 부경대학교 전자계산학과 (이학석사)
2000년 부경대학교 전자계산학과 (이학박사)
2000년~2001년 한국정보통신대학교 Post-Doc.
2001년~2005년 한국전자통신연구원 디지털방송연구단 선임연구원
2005년~2006년 경성대학교 컴퓨터정보학부 초빙교수
2013년~2014년 공주대학교 Post-Doc.
2014년~2015년 숭실대학교 전임연구원
2015년~현재 부경대학교 전임연구원
관심분야 : 디지털 저작권 관리, 멀티미디어 보안, 클라우드 컴퓨팅

이 석 환

1999년 경북대학교 전자공학과 학사 졸업(공학사)
2001년 경북대학교 전자공학과 석사 졸업(공학석사)
2004년 경북대학교 전자공학과 박사 졸업(공학박사)
2005년~현재 동명대학교 정보보호학과 부교수
2010년~현재 IEEE R10 창원섹션 임원
관심분야 : 워터마킹, DRM, 영상신호처리

권 기 룡

1986년 경북대학교 전자공학과 학사 졸업(공학사)
1990년 경북대학교 전자공학과 석사 졸업(공학석사)
1994년 경북대학교 전자공학과 박사 졸업(공학박사)
2000년~2001년 Univ. of Minnesota, Post-Doc.
1996년~2006년 부산외국어대학교 디지털정보공학부 부교수
2006년~현재 부경대학교 IT융합응용공학과 교수
2011년~2012년 Colorado State Univ., Visiting Scholar
2011년~2016년 IEEE R10 창원섹션 의장
2015년~2016년 한국멀티미디어학회 회장
관심분야 : 멀티미디어정보보호, 영상처리, GIS 보안, 드론, 3D 프린팅

박 윤 경

1987년 고려대학교 수학교육학과 졸업(이학사)
2006년 충남대학교 정보통신공학과 졸업(공학석사)
1987년~1997년 한국전자통신연구원 연구원
1998년~2004년 한국전자통신연구원 선임연구원
2005년~현재 한국전자통신연구원 책임연구원
관심분야 : 추천시스템, 인공지능, 상황인지

문 경 덕

1990년 2월 한양대학교 전산학과 (공학사)
1992년 8월 한양대학교 전산학과 (공학석사)
2005년 2월 KAIST 정보공학(공학박사)
1992년~1997년 시스템공학연구소 연구원
1997년~2005년 한국전자통신연구원 선임연구원
2005년~현재 한국전자통신연구원 책임연구원
관심분야 : 지능형 홈네트워크, 스마트그리드, 감성ICT, 자율컴퓨팅, 콘텐츠 처리