

2019 한국정보보호학회 동계학술대회

CISC-W'19

Conference on Information Security and Cryptography-Winter 2019

일시 2019. 11. 30(토)

장소 중앙대학교(흑석동)

Proceedings



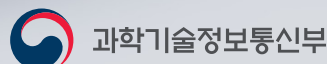
주최



주관



후원



구두발표 트랙 A

발표 세션	발표논문
A4 콘텐츠 보안 13:10 ~ 14:10 좌장 곽 진(아주대)	음악 스트리밍 프로파일링 기반의 불법 음악 스트리밍 사이트 탐지 방안 정혜선, 곽진(아주대)
	공공 인프라 영상보안을 위한 보안 프레임워크 연구 유진용, 김영갑(세종대)
	클라우드 공유 기능의 저작권 침해 방지를 위한 연구 박소희, 곽진(아주대)
	공공장소 CCTV 프라이버시 확보 기법 권혁동, 장경배, 권용빈, 서화정(한성대)

튜토리얼	발표논문
차세대인증 14:20 ~ 15:20 좌장 최대선(공주대)	DID 개념과 영지식 증명 황정연 박사(ETRI)

클라우드 공유 기능의 저작권 침해 방지를 위한 연구

박소희*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

The Prevention of Copyright Infringement in Cloud Sharing Function

So-Hee Park*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University.

**Department of Cyber Security, Ajou University.

요약

클라우드의 사용자의 요구 및 수요 변화에 따라 데이터를 시간과 장소에 제약받지 않으며 신속적으로 이용할 수 있도록 하는 정보처리체계이다. 매년 클라우드 데이터센터 트래픽은 증가하고 있으며 클라우드 내에 주요정보를 저장하는 개인 사용자 및 기업 또한 늘고 있는 추세이다. 또한 공유된 데이터를 언제 어디서나 다운로드할 수 있는 환경이 형성되면서 사용자의 편리성이 증대되었다. 그러나 클라우드 내에서 발생하는 공유된 데이터의 저작권 침해 행위가 증가하는 반면 이에 대한 대응은 미흡하다. 따라서 클라우드 환경에 적용할 수 있는 보안 서비스에 대한 연구가 필요하다. 본 논문에서는 데이터 유출 방지 기반 모듈을 구성하여 클라우드 환경에서 저작권 침해 행위를 대응하기 위한 아키텍처를 연구한다.

I. 서론

클라우드(Cloud)란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 사용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신속적으로 이용할 수 있도록 하는 정보처리체계이다[1].

클라우드의 비용 절감, 업무 효율성 및 생산성 향상 효과 등을 가진다. 클라우드 데이터센터 트래픽이 2016년 기준 연간 6.0ZB에서 2021년에는 19.5ZB까지 연평균 27%의 성장률을 보일 것이며, 2021년 전체 데이터센터 트래픽의 95%를 차지할 것으로 전망되고 있다[2]. 또한 최근 클라우드 내에 주요정보를 저장하는 개인 사용자·기업이 늘고 있는 추세이다.

클라우드 서비스가 증가하면서 공유되는

데이터를 언제 어디서나 다운로드할 수 있는 환경이 형성되었다. 클라우드 서비스는 사용자의 편리성을 추구하지만 이를 이용한 저작권 침해 행위 또한 증가하고 있다. 그러나 클라우드 환경에서의 저작권 침해에 대한 인식 및 대응 방안은 부족한 실정이다. 따라서 클라우드 환경에서 활용 가능한 보안 서비스 제공을 위해 다양한 연구가 필요하다.

본 논문에서는 데이터 유출 방지 (DLP, Data Loss Prevention) 기반 모듈을 구성하여 클라우드 환경에서 발생 가능한 저작권 침해 행위에 대응하기 위한 아키텍처를 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드 저작권 및 데이터 유출 방지에 대하여 연구하고, 3장에서 저작권 침해 행위에 대한 시나리오를 분석한다. 4장에서 보안 서비스를 적용한 클라우드 아키텍처에 대하여

본 연구는 문화체육관광부 및 한국저작권위원회의 2019년도 저작권기술개발사업의 연구결과로 수행되었음.

분석하고 5장에서 결론을 내린다.

II. 클라우드에 의한 저작권 침해

2.1 클라우드 저작권 침해 유형

저작권법은 저작자의 권리와 이에 인접하는 권리를 보호하고 저작물의 공정한 이용을 도모함으로써 문화 및 관련 산업의 향상발전을 목적으로 한다[3]. 저작권법의 목적이 문화 및 관련 산업의 향상발전에 있는 만큼 저작권을 지적재산으로 인정하기 때문에 저작자가 아닌 자가 저작물로서 영리를 목적으로 할 때 저작자의 권리를 해한 것으로 간주하며 해당하는 행위를 제재한다.

저작권법 제27조에 따르면 저작자가 아닌 자가 공표된 저작물을 영리를 목적으로 하거나, 가정 및 이에 준하는 한정된 범위를 넘어서 불특정 다수와 복제한 저작물을 이용하는 경우 이는 사적이용을 위한 복제가 아니므로 저작권 침해에 해당한다[3]. 따라서 정당한 값을 지불하지 않은 자에게 저작물을 이용할 수 있는 권리를 부여하는 것은 클라우드 서비스에 의한 저작권 침해 행위이다. 클라우드 서비스의 아이디 및 패스워드를 불특정 다수인과 공유하는 경우, 저작물이 업로드된 폴더에 불특정 다수인을 멤버로 초대하는 경우, 저작물을 다운받을 수 있는 링크를 생성하여 저작물을 타인에게 배포하는 경우 등으로 저작권 침해 유형을 나눌 수 있다.

따라서 사용자가 저작물을 클라우드에 업로드 할 때, 다른 사용자와 저작물 공유를 위한 배포 경로의 모니터링과 사적 복제의 가능 여부를 확인하여 저작권 침해 행위를 판별할 수 있다. 본 논문에서는 배포 경로의 감시와 사적 복제의 가능 여부 확인을 위해 클라우드 환경 보안 서비스 모듈에 DLP 시스템을 사용한다.

2.2 데이터 유출 방지 (Data Loss Prevention)

데이터 유출 방지는 정보 유출을 막기 위해 콘텐츠의 이동을 모니터링하며 이동하는 데이터에 기밀정보 및 개인정보 등 주요정보가

포함되어 있을 경우 이를 차단하여 데이터를 보호한다. 구성원과 프로세스 및 기술의 결합을 통해 주요정보가 외부로 유출되는 것을 방지한다. 사용되는 데이터를 위한 데이터 유출 방지는 사용자 인증과 자원에 대한 액세스를 제어하고 응용 프로그램이나 엔드포인트에 의해 처리되는 데이터를 수집한다. 이동되는 데이터를 위한 데이터 유출 방지는 주요정보가 네트워크를 통해 전송되는 경우 외부로의 주요정보 라우팅 여부와 저장소 영역의 안전 여부에 대해 확인한다. 유희 데이터를 위한 데이터 유출 방지는 권한을 가진 사용자만 데이터에 액세스할 수 있도록 하고 데이터가 유출될 경우 액세스를 추적하는 기능 등으로 클라우드를 포함한 다양한 저장 매체의 데이터를 보호한다[4].

III. 저작권 침해 시나리오

[그림 1]은 클라우드 환경에서 사용자가 저작물 공유를 통해 저작권을 침해하는 과정에 대하여 나타낸 것이다. 과정은 다음과 같다.



[그림 1] 저작권 침해 시나리오

Step 1. 클라우드 사용자의 저작물 업로드

사용자가 클라우드 서버에 저작물을 업로드한다. 사용자 본인이 업로드한 저작물의 저작자일 경우 특정·불특정 다수인과 클라우드 서비스를 이용하여 공유하는 것은 저작권법상 문제가 되지 않는다. 그러나 저작자가 아닐 경우에 저작권 침해의 우려가 있다.

Step 2. 제3자 대상의 저작물 배포

사용자가 클라우드의 공유 기능을 통하여 불특정 다수인과 저작물을 공유하며 클라우드

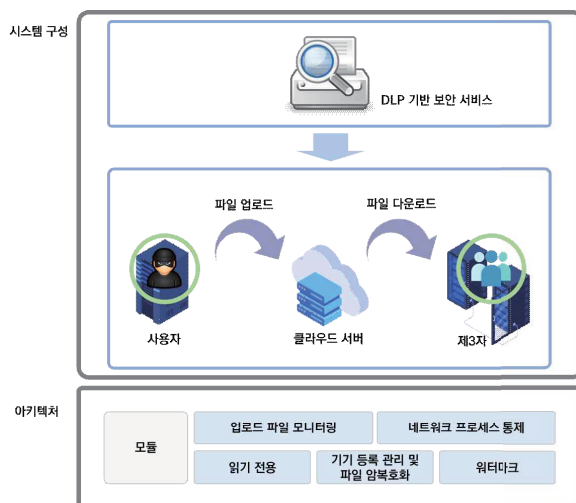
환경에서 저작권 침해는 대부분 이와 같은 형태이다. 따라서 클라우드에 저작물을 업로드하는 행위는 저작권 침해가 일어나는 원인이다. 그러나 클라우드의 정의에 따르면 언제 어디서나 필요한 파일을 다운로드 할 수 있는 서비스로써 해당 행위를 제한하는 것은 클라우드의 정의와 맞지 않는다.

Step 3. 저작물 공유로 인한 저작권 침해

제3자가 정당한 대가를 지불하지 않고 저작물을 다운로드 받음으로써 저작권을 침해한다.

IV. 제안 사항

클라우드 환경에서 일어나는 저작권 침해를 방지하기 위해서 저작물의 업로드를 제한하는 것은 클라우드의 정의와 맞지 않기 때문에 불가능하다. 클라우드에 동시 접속할 수 있는 기기의 수를 제한하거나 사용자가 기기를 등록하여 클라우드에 대한 이용을 제한하는 등의 방법이 사용되고 있다. 그러나 논문에서 다루는 클라우드 서비스의 분류상 저장 공간 제공이라는 특성 때문에 데이터 복제 및 다운로드 등의 서비스 이용에 대한 저작권 침해를 막을 수 없다. 따라서 저작물의 통신상 이동에 중점을 두고 데이터 유출 방지 솔루션을 사용하여 클라우드 보안 서비스를 제공할 때 필요한 기능을 제안한다.



[그림 2] 제안하는 클라우드의 공유 기능에 의한 저작권 침해 행위 대응 아키텍처

본 절에서는 [그림 2]의 구성으로 데이터 유출 방지 기반의 클라우드 저작권 침해를 방지하는 보안 서비스 아키텍처를 제안한다. 보안 서비스 아키텍처는 다음과 같은 기능을 가진다.

4.1 업로드 파일 모니터링

클라우드에 업로드되는 모든 파일에 대한 암호화된 데이터를 저장한다. 또한 파일의 헤더값을 비롯한 위변조 발생을 모니터링하며 위변조를 발견할 경우 파일 업로드에 제재를 둔다.

4.2 네트워크 프로세스 통제

화이트 리스트 (White List) 방식으로 사전에 프로세스를 등록하여 허용된 프로세스에 대한 정책을 설정한다. 등록된 프로세스는 사용자가 주로 접속하는 IP주소 정보로 프로세스에 따라 파일의 업로드와 다운로드에 대한 허용 및 차단 설정을 관리하며 모든 업로드된 파일을 모니터링한다. 해당 로그를 수집하여 프로세스가 등록된 화이트 리스트에 항목을 추가하거나 삭제한다.

4.3 읽기 전용

클라우드 환경의 저작물이 업로드된 폴더를 이용하는 공유 기능에 대하여 제한을 설정한다. 읽기 전용 서비스로써 업로드된 파일의 다운로드, 편집 및 저장이 불가하며 웹을 이용한 파일의 열람이 가능하다.

4.4 기기 등록 관리 및 파일 암호화

클라우드를 사용하는 기기를 미리 등록한다. 또한 클라우드에 저장되는 모든 파일을 자동 암호화한다. 등록된 기기를 통한 서비스 이용만을 가능하게 하며 등록된 기기가 아닐 시 암호화된 파일의 열람이 불가하다.

4.5 워터마크

클라우드에 업로드된 파일을 다운받을 경우 워터마크를 함께 출력한다. 로고 이미지, 저작자 정보, 저작물에 대한 명시 등의 정보를 표시한다.

[표 1] 제안하는 클라우드의 공유 기능에 의한 저작권 침해 행위 대응 아키텍처의 기능

모듈	설명
업로드 파일 모니터링	- 업로드 파일 모니터링 및 위변조 파일 업로드 제한 - 저작권 침해 방지에 대한 우회 탐지를 통해 저작권을 보호함
네트워크 프로세스 통제	- IP주소 정보 수집 및 프로세스 정책 설정 - 저작물 공유 정책의 강화를 통해 저작권을 보호함
읽기 전용	- 공유 기능의 파일 이용 제한 - 저작물의 재배포 방지를 통해 저작권을 보호함
기기 등록 관리 및 파일 암복호화	- 사용자 기기 등록 및 파일 암호화 - 저작물 사용 정책의 강화를 통해 저작권을 보호함
워터마크	- 파일 대상 워터마크 출력 - 저작권에 대한 확고한 명시를 통해 저작권을 보호함

V. 결론

최근 클라우드 서비스 기술이 지속적으로 발전함에 따라 클라우드 내에 주요정보를 저장하는 개인 사용자·기업이 늘고 있는 추세이다. 클라우드 서비스 사용이 증가하면서 클라우드 환경에서 발생하는 보안 위협에 대한 연구가 지속되고 있다. 본 논문에서는 클라우드 서비스를 통한 저작권 침해 유형에 대해 분석하였다. 또한 저작권 침해 행위의 방지를 위하여 데이터 유출 방지 기반 모듈로 구성된 클라우드 환경의 보안 서비스 아키텍처를 제안하였다. 클라우드 환경에서 저작물의 배포 경로를 모니터링하고 사적 복제의 가능 여부를 확인하기 위해 데이터 유출 방지 기술을 사용하였으며 제안한 모델을 보안 서비스로 제공할 경우 클라우드 보안 서비스에 필요한 복합적인 요소를 고려하여 저작권에 대한 보호가 이루어질 것이다.

향후, 제안한 모델의 연구 및 구현을 통해 기능을 개선하고, 실제 서비스 제공시 효율성 및 안전성을 보장할 수 있는 시스템에 대한 연구가 지속될 것이다.

[참고문헌]

- [1] 과학기술정보통신부, “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률”, July, 2017.
- [2] 한국인터넷진흥원, “클라우드 정보보호 안내서”, December, 2017.
- [3] 문화체육관광부, “저작권법”, October, 2018.
- [4] Cisco, “What Is Data Loss Prevention(DLP)?”, October, 2019.