클라우드 컴퓨팅 기반 스트리밍 서비스(StraaS)의 설계

Design of StraaS(streaming as a service) based on Cloud Computing

차병래*, 심수정**, 김용일***

Byung-Rae Cha*, Su-Jeong Sim*, and Yong-Il Kim**

요 약

본 논문에서는 클라우드 컴퓨팅 기반의 스트리밍 서비스를 제공하기 위한 Streaming as a Service(StraaS)를 정의하며, StraaS 서비스를 제공하기 위한 다양한 기능과 보안에 대해서 기술한다. 특히 클라우드 컴퓨팅과 스트리밍 서비스를 위한 보안 기능으로 KS-MMA(Key-generation System for Multilateral Matching Authentication) 그리고 SIES(Searchable Image Encryption System)에 대해서 기술한다.

Abstract

In this paper, we define and design the Streaming as a Service (StraaS) to support streaming service based on cloud computing. And we describe the various function and security to StraaS service. Specially, we introduce KS-MMA(Key-generation System for Multilateral Matching Authentication) and SIES(Searchable Image Encryption System) as security function for streaming service and cloud computing.

Key words : Streaming, StraaS, Cloud Computing

I. 서 론

최근 IT 분야의 이슈를 보면, 클라우드 컴퓨팅과 빅 데이터(Big Data)가 여러 이슈들 중에 포함되어 있으며, 산·학·연 활동이 활발히 진행 중에 있다. 컴퓨팅 환경 분야의 새로운 패러다임으로 클라우드 컴퓨팅(Cloud Computing)이 거론되고 있으며, 활발한 소셜 네트워킹(Social Networking)에 의한 빅 데이터가 새로운 이슈로 부각되었다. 이 두 영역에 위치한 서비스 중의 하나가 스트리밍 서비스이며, 스트리밍 서비스에 의해서 빅 데이터 문제와 이에 관련된 문제점들이 새로이 대두되고 있다. 클라우드 컴퓨팅을 구성하는 다양한 기술에 의해서 이러한 문제점들을 극복하기 위한 클라우드 컴퓨팅 기반의 스트리밍 서비스를 설계하고자 한다. 본 연구의 목표는 클라우드 컴퓨팅 기반의 스트리밍 서비스를 지원하기 위한 StraaS(Streaming as a Service) 설계이다.

검색 가능 암호 시스템(SES; Searchable Encryption System)은 암호화된 자료를 복호화하지 않고도 원하는 자료를 검색할 수 있도록 하는 암호 기반 기술이다. 검색 가능 암호 시스템은 개인의 정보가 외부 저장 공간에 저장되면서 발생하는 여러 문제점에 대한

* 광주과학기술원(GIST.)
** 전남대학교 (Chonnam University)
*** 호남대학교 (Honam University)
· 제1저자 (First Author) : 차병래
· 투고일자 : 2012년 3월 7일
· 심사(수정)일자 : 2012년 3월 8일 (수정일자 : 2012년 4월 18일)
· 게재일자 : 2012년 4월 30일

해결 방법으로 지금까지 많은 연구가 진행되었다. 최근 기업 데이터베이스에서의 고객 정보 유출 사례나 개인 홈페이지에 저장된 사진 등의 개인 정보의 유출 사례가 보고되면서, 이러한 외부 저장 공간에 저장되어 있는 정보에 대한 보안 문제가 이슈가 되고 있다. 외부 저장 공간에서의 보안 문제는 과거 개인이 독립된 저장 공간을 이용하여 스스로 정보를 관리하던 때와는 차이를 보인다. 이는 근본적으로 정보의 소유자와 저장 공간을 관리하는 주체가 서로 다르기 때문이다. 데이터베이스 등에서 정보를 보호하기 위해 주로 사용되는 접근 제어나 키 관리 기법들은 외부 침입자를 막는 데 유효한 방법이지만 저장 공간의 소유자가 저장되어 있는 자료를 열람하는 것을 근본적으로 방지하지 못한다.

본 논문의 2장은 빅 데이터a, 클라우드 컴퓨팅, 스케일 아웃에 관한 관련 연구를 기술한다. 3장에서는 클라우드 기반의 StraaS 서비스를 설계하며, 4장에서는 StraaS 서비스의 보안, 5장에서는 StraaS의 응용 및 비즈니스 모델에 대해 기술하며, 간략하게 결론으로 구성되었다.

Ⅱ. 관련 연구

2-1 Big Data

기업마다 빅 데이터의 형태나 요구 사항은 매우 다양하고, 이에 따른 컴퓨팅 환경도 복잡해졌다. 특히 스토리지 입장에서는 단순히 데이터를 저장하는 것뿐만 아니라, 다양한 컴퓨팅 환경을 유기적으로 연동시켜야 한다는 점에서 가장 중요한 인프라이며, 전체 컴퓨팅 환경을 결정짓는 핵심 요소이다. 그림 1은 빅 데이터의 3요소인 크기(Volume), 속도(Velocity), 그리고 다양성(Various)을 나타낸 것이다. McKinsey [1]의 “Big Data: The next frontier for innovation, competition, and productivity”에서 매달 300억 개의 콘텐츠가 Facebook에서 공유되고, 전 세계 데이터는 매년 40% 증가, IT 지출은 5% 증가하고 있으며, Big Data 활용 시 미국 의료 분야에서 매년 3,300억 달러 가치 생산 가능 (연간 스페인 전체 의료 지출 비의 2배 이상), 유럽 공공 분야에 활용 시 2,500억 유로 절감 효과 (그리스 GDP 규모), 2018년까지 미국에서만 14 ~ 19만 명의 분석 전문 인력과 150만 명의 데이터 관리자에 대한 수요가 발생할 수 있다고 언급했다.

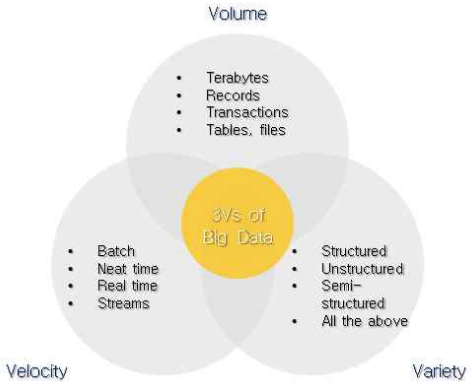

그림 1. Big Data의 3요소
Fig. 1. 3 components of big data

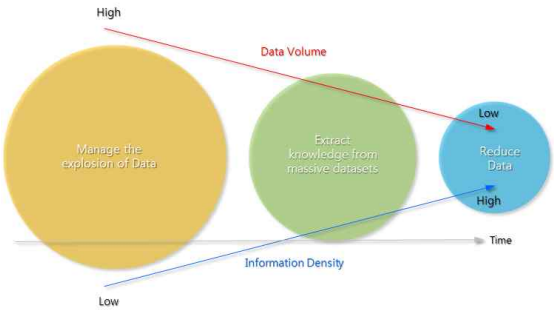

그림 2. Big Data의 가치 창출
Fig. 2. Value creation of big data

빅 데이터와 관련된 모든 영역에서 클라우드 컴퓨팅 기술을 이용하면 빅 데이터의 효율적 활용과 가치 창출이 가능하며, 특히 클라우드 컴퓨팅 기반의 하둡(Hadoop), 맵리듀스(MapReduce) 같은 솔루션이 빅 데이터의 복잡성 문제를 해결할 수 있다. 또한 그림 2와 같이 클라우드 컴퓨팅 시스템의 풍부한 컴퓨팅 자원과 네트워크 강화(scaling of network)에 의해서 빅 데이터의 실시간 분석이 가능하며, 새로운 가치를 창출할 수 있는 기반을 조성할 수 있다. 또한 기존 유무선 네트워크 및 주파수 인프라 관리도 복잡하고 다양한 빅 데이터에 맞게 대응할 수 있는 다양한 기술들이 필요하다.

2-2 클라우드 컴퓨팅 패러다임

가트너(Gartner)[2] 그룹은 매년마다 다음 해에 선도할 10대 전략 기술에 대한 동향을 발표하고 있으며, 향후 3년을 기준으로 가장 잠재력 있는 전략기술이 무엇인지 선정하여 발표하며, 최근의 동향은 그림 3과 같다.

	2008	2009	2010	2011
1	Green IT	Virtualization	Cloud Computing	Cloud Computing
2	Unified Communications	Business Intelligence	Advanced Analytics	Mobile Applications and Media Tablet
3	Business Process Management	Cloud Computing	Client Computing	Social Communication and Collaboration
4	Metadata Management	Green IT	IT for Green	Video
5	Virtualization	Unified Communications	Reshaping the Data Center	Next-Generation Analytics
6	Mashup	Social S/W and Social Networking	Social Computing	Social Analytics
7	Web Platform	Web Oriented Architecture	Security-Activity Monitoring	Context-Aware Computing
8	Computing Fabric	Enterprise Mashups	Flash Memory	Storage Class Memory
9	Real World Web	Specialized Systems	Virtualization for Availability	Ubiquitous Computing
10	Social Software	Servers-Beyond Blades	Mobile Applications	Fabric-Based Infrastructure and Computers

그림 3. 가트너 그룹의 연차별 10대 전략 기술
Fig. 3. Annual 10 strategy techniques of Gartner group

클라우드 컴퓨팅은 컴퓨터 리소스(Resource)를 가상화(Virtualization)하고 통합하여, 사용자가 필요할 때 필요한 만큼 리소스를 할당 받고 데이터를 손쉽게 공유할 수 있는 컴퓨팅 환경이다. 클라우드 서비스의 출현은 다시한번 IT의 경제성을 근본적으로 변화시키고 있다. 클라우드 기술은 IT 리소스를 표준화하고 통합하며 오늘날 수동으로 이루어지는 많은 작업들이 자동화되고 있다. 클라우드 아키텍처는 탄력적인 소비, 셀프 서비스 그리고 사용량만큼 지불하는 모델을 지원한다. 이 외에도 클라우드는 핵심 IT 인프라를 대규모 데이터 센터로 가져와 다음과 같은 세 가지 부문에서 우수한 규모의 경제를 달성할 수 있도록 지원한다.

- 공급 측 절감: 대규모 데이터 센터(DC)의 서버당 비용이 절감된다.
- 수요 측 집계: 컴퓨팅에 대한 총 수요가 전반적인 변동성을 원활하게 하여 서버 활용도가 높아진다.
- 멀티테넌시(Multi-tenancy)효율성: 멀티 테넌트 응용 프로그램 모델로 변경할 때, 테넌트의 수(예, 고객 또는 사용자)가 증가하게 되어 테넌트 별 응용 프로그램 관리 및 서버 비용이 절감된다.

클라우드 컴퓨팅의 서비스는 IaaS(Infrastructure asa a Service), PaaS(Platform as a Service), 그리고 SaaS(Software as a Service)라 하며, 특정한 업무 X에 의해서 XaaS(X-as a Service)라고 명칭하기도 한다. 특정한 업무가 Database이라면 DaaS (Database as a Service), Network이라면 NaaS (Network as a Service)라 명명한다. 본 연구에서는 Streaming as a Service라는 의미로 StraaS를 명명한다.

2-3 스트리밍 서비스를 위한 스케일 아웃 기술

오늘날 전 세계적으로 수백만의 사용자들을 대상으로 하는 소셜 네트워크, 개인 데이터 공유 및 백업, IPTV, 비디오 스트리밍 서비스 등에서 발생되는 대용량 콘텐츠가 증가하고, 모바일 기기의 수요 증가에 따라 생성되는 비정형화된 데이터 트래픽 역시 폭발적으로 증가하여, 스토리지 시장에 새로운 발판을 마련하고 있다. 예측이 불가능하고 폭발적으로 증가하는 파일 기반의 비 정형화된 데이터를 빅 데이터라 부르며, 이러한 빅 데이터를 잘 관리할 수 있는 스토리지 기술 중의 하나가 바로 스케일 아웃 기술이다. 여러 RAID(Redundant Array of Independent Disks) 스토리지 시스템에 단지 클러스터링 기술만 적용한 제품이나, 확장에 제한이 있는 파일 시스템과 볼륨들로 구성된 환경에 유틸리티 기술을 적용한 제품을 스케일 아웃 방식의 스토리지라 부르기에는 다소 부족한 부분이 있다. 스케일 아웃 스토리지의 기본 개념은 서비스 중단 없이 스토리지 리소스를 추가함으로써, 성능과 용량 그리고 처리량을 선형적으로 증가시킬 수 있어야 한다. 그러나 단순히 여러 개의 볼륨을 합쳐 하나의 파일 시스템처럼 보여주는 구조는 폭발적으로 데이터가 증가하는 빅 데이터 환경에서는 스토리지의 용량 및 성능의 한계뿐만 아니라 관리적인 측면에서 복잡해질 수 있다.

2-4 검색 가능 암호 시스템의 기술 동향

정보를 안전하게 저장하기 위한 다른 방법으로 암

호화를 생각할 수 있다. 즉, 외부 저장 공간에 저장할 정보를 안전성이 증명된 암호 시스템을 이용하여 암호화하는 것이다. 안전성이 증명된 암호 시스템은 복호화 키를 소유하지 못한 공격자가 암호문으로부터 실제 저장된 정보를 얻을 수 없다는 것을 보장한다. 따라서, 외부 침입자 또는 저장 공간의 소유자가 외부 저장 공간에 저장된 암호문에 접근했다하더라도 실제 의미 있는 정보를 얻지는 못한다는 것을 의미한다. 정보의 암호화는 저장된 정보의 유출을 완벽하게 방지하는 방법이지만, 기존 데이터베이스가 제공하는 많은 부가 기능 또한 적용할 수 없도록 만든다. 저장된 정보의 양이 많을수록 이를 효율적으로 활용하고 정리하기 위해서 다양한 데이터베이스 기능이 요구되기 때문에 단순히 정보를 암호화하여 저장하는 방법은 적당한 해법이라 보기 힘들다.

검색 가능 암호 시스템(SES)은 기존의 암호 기술과 같이 암호화된 정보에 대한 안전성을 보장하면서 동시에 특정 키워드를 포함하는 정보를 검색할 수 있도록 고안된 암호 기술이다. 데이터베이스에서 제공되는 다양한 기능 중 많은 경우가 특정 키워드를 포함하는 정보에 대한 검색을 바탕으로 이루어지기 때문에 검색 가능 암호 시스템은 앞에서 제기된 문제에 대한 해결 방안 중 하나로 여겨지고 있다. 또한 기본적인 검색 이외에도 범위 검색, 결합(conjunctive) 검색 등의 다양한 검색 기능을 제공하는 검색 가능 암호 시스템[3 - 6]에 대한 연구도 진행 중이다.

검색 가능 암호 시스템에서 암호화의 대상인 정보를 문서(Document)라 부른다. 즉, 문서는 사용자가 숨기고 싶은 정보(Information)이다. 또한, 사용자가 자신이 원하는 문서를 검색하기 위해 서버에 제공하는 정보를 키워드(keyword)라고 부른다. 일반적으로 자료는 그 문서에 포함된 키워드들의 집합으로 (1)과 같이 정의된다.

$$D = \{ W_1, W_2, \cdots, W_n \} \qquad (1)$$

검색 가능 암호 시스템은 키 생성(key generation), 암호화 및 색인(build index), 트랩도어 생성(trapdoor generation), 검색(search)의 4가지 단계로 이루어지며, 그림 4와 같이 나타낸다.

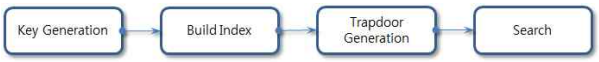

그림 4. 검색 가능 암호 시스템의 기본 구성
Fig. Basic structure of searchable encryption system

검색 가능 암호 시스템은 다음과 같은 요구 조건을 만족시켜야 한다. 우선 검색 단계에서는 주어진 트랩 도어와 일치하는 모든 문서들이 검색되어야 하며, 검색에서 발생할 수 있는 오류는 최소화되어야 한다. 여기에서 오류란 주어진 트랩 도어에 대응하는 키워드를 포함하고 있지 않은 문서가 검색 결과에 포함될 확률을 의미한다. 정보 보호 측면에서 볼 때, 검색 과정에서 유출되는 정보의 양은 가능하면 작아야 한다. 좀 더 구체적으로 주어진 트랩 도어와 관계없는 또는 일부 키워드만을 포함하는 문서에 대한 정보는 유출이 되어서는 안된다.

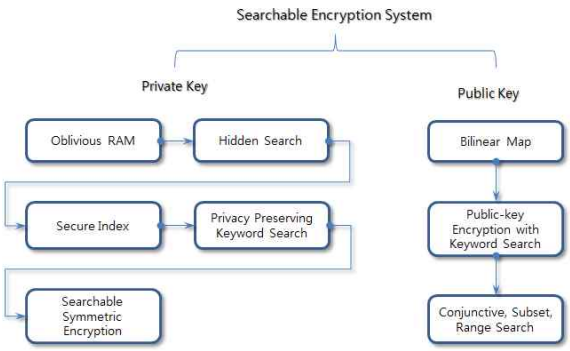

그림 5. 개인 키와 공개 키에 의한 SES 분류
Fig. 5. SES classification by private key and public key

검색 가능 암호 시스템은 개인의 정보가 외부 저장 공간에 저장되면서 발생하는 여러 문제점에 대한 해결 방법으로 지금까지 많은 연구가 진행되었으며, 그림 5와 같이 사용자의 암호화 키에 의해 공개 키 방식과 개인 키 방식으로 분류할 수 있다. [7]

Ⅲ. StraaS의 설계

클라우드 컴퓨팅 기반과 데이터 처리 기술을 이용하여 스트리밍 서비스를 제공하는 것을 StraaS (Streaming as a Service)라 정의하며, 그림 6과 같이 나타낸다.

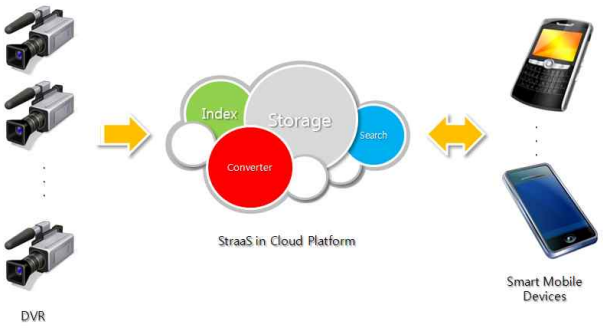

그림 6. StraaS의 개념 다이어그램
Fig. 6. Concept diagram of StraaS

3-1 Streaming as a Service의 시스템 설계

StraaS는 기존의 스트리밍 서비스를 클라우드 컴퓨팅 인프라의 컴퓨팅, 네트워킹, 그리고 스토리지 자원위에서 보안을 제공하며, 다양한 서비스를 위한 데이터 처리 기술을 서비스로 제공하는 서비스를 의미한다. 스트리밍을 서비스하기 위한 StraaS의 시스템 구성은 그림 7의 IPO 모델로부터 그림 8의 개념도를 도출한다. IPO 모델은 데이터(Data)를 정보(Information)로 가공하기 위한 입력(Input), 처리(Processing), 저장(Storage), 그리고 출력(Output)으로 구성되는 정보 가공을 위한 개념도이다.

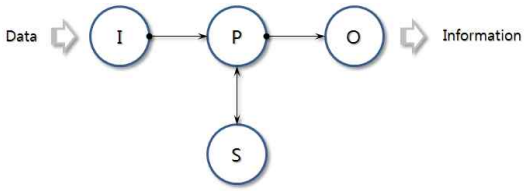

그림 7. IPO 모델
Fig. 7. IPO Model

StraaS 서비스를 제공하기 위해서는 가장 먼저 클라우드 컴퓨팅의 컴퓨팅, 네트워킹, 그리고 스토리지 자원이 필요하다. 클라우드의 네트워킹 자원은 스트리밍 서비스 제공하기 위한 생성된 스트리밍 미디어의 근원지와 소비하는 목적지, 그리고 클라우드의 컴퓨팅 장치 및 스토리지의 연결을 담당한다. 클라우드의 컴퓨팅 자원은 스트리밍 미디어의 변환, 인증 및 암호/복호화 등의 프레임워크에서 제공하는 서비스를 지원한다. 클라우드의 스토리지 자원은 스트리밍 미디어를 저장하기 위한 공간을 제공하며, 특히 서비스를 위한 저장 공간인 퍼블릭 클라우드(public cloud)의 스토리지(storage)와 아카이브(archive)를 위한 저장 공간으로 프라이빗 클라우드(private cloud) 의 스토리지로 구분한다.

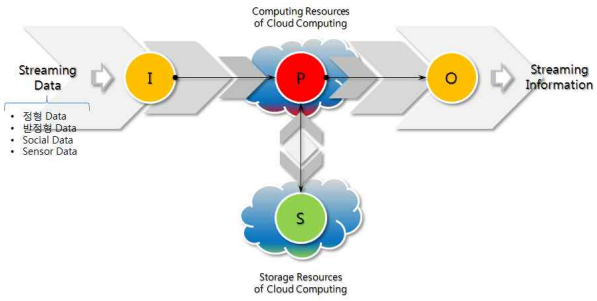

그림 8. StraaS 시스템 개념도
Fig. 8. System concept of StraaS

3-2 StraaS의 서비스 기능

StraaS는 클라우드 컴퓨팅 기반의 스트리밍 서비스를 제공하며, 임의의 제약조건에서도 클라우드의 컴퓨팅을 탄력적으로 운용하여 스트리밍 미디어의 변환, 색인/검색 및 압축 등의 다양한 서비스를 실시간으로 제공할 수 있다는 것이 StraaS의 특징이다.

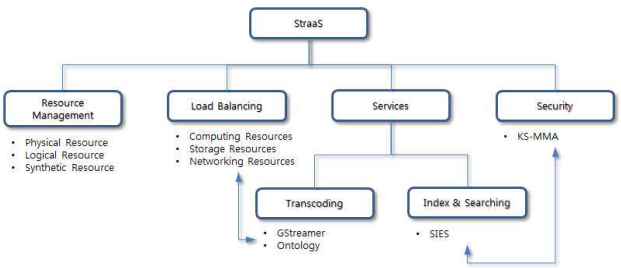

그림 9. StraaS 서비스의 기능도
Fig. 9. Function diagram of StraaS Service

3-3 변환 (Transcoding)

StraaS는 스트리밍 미디어의 데이터 센터 역할을 수행한다. 여러 곳에서 생성된 다양한 스트리밍 미디어들과 스트리밍 미디어를 소비하는 디바이스의 자원을 인지하여 알맞은 스트리밍 미디어 포맷을 클라우드의 컴퓨팅 자원을 이용하여 실시간 변환 기능을 제공한다. 스트리밍 미디어의 변환은 오픈 소스인 GStremer tools [8]을 이용하여 개발하며, 그림 10에 GStreamer의 개요를 나타낸다.

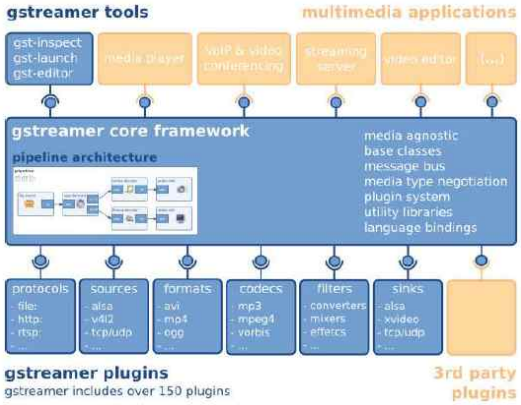

그림 10. GStreamer의 개요
Fig. 10. Overview of GStreamer

3-4 색인 및 패턴 정보

StraaS는 실시간으로 생성된 스트리밍 미디어를 분석하여 다양한 색인 및 정보를 생성한다. 이 데이터 처리과정에서는 색인과 패턴 정보가 생성된다. 색인은 스트리밍 미디어를 클라우드의 컴퓨팅 자원을 이용하여 이미지 프로세싱을 수행하여 생성되며, 색인 외에 생성된 추가정보를 이용하여 패턴 정보를 생성한다. 이와 같은 절차를 그림 11에 나타낸다.

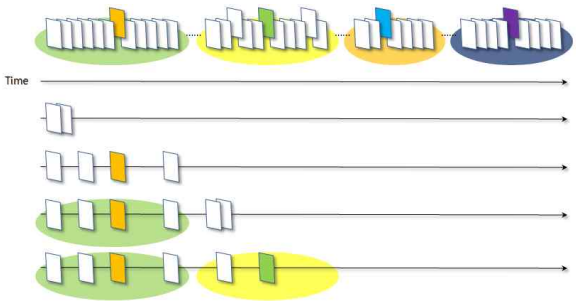

그림 11. Partial story cut의 과정
Fig. 11. Process of partial story cut

색인 정보(Index information)는 크게 포스터 컷(Poster Cut)과 부분 스토리 컷(Partial Story Cut)으로 구성된다. Partial Story Cut은 이미지 처리(Image Processing)에 의해서 스트리밍 미디어를 영역 설정 및 분할하며, 분할된 스트리밍의 평균에 해당하는 이미지를 선택하는 과정이며, 그림 12와 같이 나타낼 수 있다. 그리고 Poster Cut은 Partial Story Cut의 평균 이미지를 타일 형태의 디스플레이(Tiled Display) 형태로 스트리밍 미디어를 요약한 정보를 추출하고, 색인을 생성한다. 특히 Poster Cut은 검색 가능한 암호화 시스템의 검색을 위한 이미지 키워드로 사용된다.

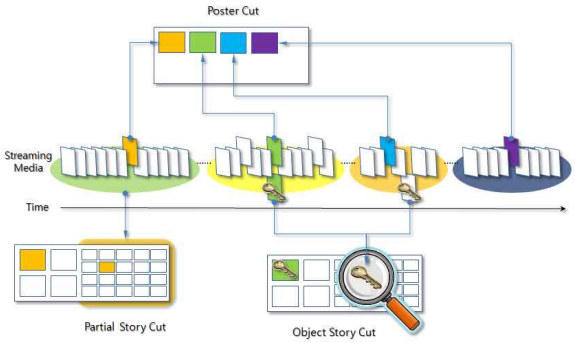

그림 12. StraaS의 색인 과정
Fig. 12. indexing process of StraaS

3-5 저장/백업 – Cloud Storage의 Scale Out 저장소

StraaS의 저장과 백업은 크게 1차 저장과 2차 저장으로 구분한다. 1차 저장은 서비스를 제공하기위한 저장소라면, 2차 저장소는 백업을 위한 저장소이다.

(1) 1차 저장 - 서비스용 스토리지

StraaS 서비스 제공하기 위한 1차 저장소로 Public Cloud인 MS의 Azure를 이용하며, 스트리밍 서비스를 제공하기 위한 컴퓨팅과 스토리지, 그리고 네트워킹을 사용한다.

(2) 2차 저장 - 아카이브용 스토리지

일정 기간 동안 사용되지 않는 스트리밍 미디어의 경우 자체 개발한 오픈 소스기반의 Private Cloud를 이용하여 백업 및 예비 기능을 수행하며, 클라우드 컴퓨팅 시스템의 오픈 소스인 OpenStack [9]을 이용하여 Private Cloud를 구축한다.

3-6 StraaS의 네트워크 및 예비 기능

StraaS의 네트워킹 및 예비(Provisioning) 기능에 대해서 기술한다.

(1) 네트워크 기능

StraaS의 원활한 운영을 지원하기 위해서는 클라

우드의 컴퓨팅 자원보다도 네트워크 자원이 우선적으로 중요하다.

(2) Provisioning 기능

StraaS의 원활한 운영을 지원하기 위한 Provisioning 기능은 크게 컴퓨팅 자원과 스토리지 자원이다.

Ⅳ. StraaS의 보안

오늘날의 컴퓨팅 환경에서 암호화의 중요성은 과거 어느 때보다 더 크다. 점점 더 많은 애플리케이션과 프로토콜이 암호화 기술을 사용하여 악의적인 공격으로부터 시스템을 보호한다. 암호화는 저장되거나 전송 중인 데이터를 보호하고, 신원 정보를 생성하고, 데이터 무결성을 확인하고, 무단 사용으로부터 콘텐츠를 보호하고, 지불 시스템을 가동하고, 2중 인증을 구현하고, 통신 도청을 방지하는 데 사용된다. 강력한 암호화는 정보의 기밀성을 보호하고 사용자, 스트리밍 서비스 또는 메시지의 합법성을 입증할 수 있다. 암호화가 취약할 경우 회사 자원 또는 기밀을 도난당하거나 경쟁에서 도태될 수 있다. StraaS의 보안 서비스는 다음과 같다.

- 스트리밍 미디어의 암/복호화
- 스트리밍 미디어의 분할/중복 저장
- KS-MMA & SIES

4-1 암호/복호화 및 분할/중복 저장

StraaS 데이터 센터에 전송된 모든 스트리밍 미디어는 컨테이너 방식으로 암호화되어 복제되고, 분할되어 스케일 아웃 스토리지에 저장된다. 스트리밍 미디어를 암호화 및 복호화를 위해서는 많은 컴퓨팅 자원이 소요된다. StraaS 서비스의 강점은 클라우드 인프라의 풍부한 컴퓨팅 자원을 사용하여 암호화 및 복호화를 실시간 처리가 가능하다.

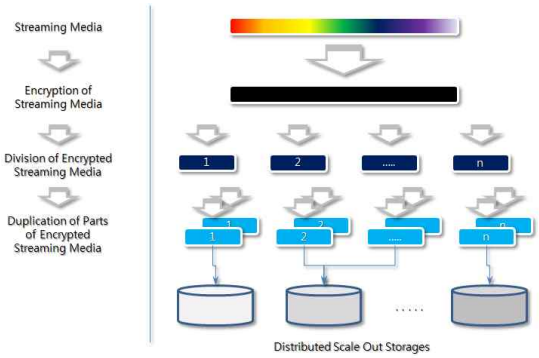

그림 13. 스트리밍 미디어의 암호화 및 분할/중복 저장

Fig. 13. Encryption and division/duplication of streaming media

(1) 스트리밍 미디어의 암호화

스트리밍 미디어의 무단 사용을 방지하기 위하여 암호화를 수행한다. 스트리밍 미디어의 생성한 측과 저장/관리하는 측이 다르기 때문에 암호화된 스트리밍 미디어의 복호화가 쌍방의 합의에 의해서만 가능하며, 이때 다자간 정합 인증을 사용하게 된다.

(2) 스트리밍 미디어의 분할 및 중복 저장

분할된 컨테이너의 스트리밍 미디어의 분실을 막기 위해서는 다중 복사하여 분산 저장 및 보관하게 된다.

(3) 스트리밍 미디어의 이미지 검색 및 복호화

암호화된 스트리밍 미디어의 무단 사용 및 접근 제어를 위하여 KS-MMA(Key-generation System for Multilateral Matching Authentication)에 의해서 인증 및 접근 제어가 가능한 경우에만 검색 및 복호화를 수행한다. 인증이 완료되고 권한이 주어지면 검색 가능한 이미지 암호 시스템에 의해서 스트리밍 미디어를 복호화하지 않고도 스트리밍 미디어의 이미지를 검색이 가능하다. 또한 암호화된 스트리밍 미디어는 분할 및 중복 분산 저장되어 있으며, 1차 검색이 실패시를 대비한, 중복 분산 저장된 스트리밍 미디어의 2차 검색이 가능하여야만 스트리밍 미디어의 완벽한 복호화가 가능하게 된다.

4-2 스트리밍 데이터의 KS-MMA

일반적인 스트리밍 미디어에 대한 접근 제어는 그림 14의 (A) 또는 (B)의 경우가 대부분의 케이스가 될 것이며, 이러한 케이스는 보안 측면의 프라이버시 문제, 디지털 저작권 관리(DRM; Digital Rights Management) 문제, 그리고 디지털 콘텐츠의 배포와 과금 등의 문제를 갖고 있다. 이러한 문제는 1차적으로 끝나지 않고 2차, 3차의 파장을 일으키고 사회적 이슈가 되고 있다. 이러한 문제점을 어느 정도 해결하기 위한 제안된 방법을 그림 15와 같다.

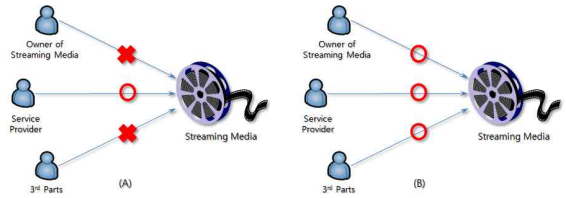

그림 14. 스트리밍 미디어의 일반적인 접근 제어
Fig. 14. General access control of streaming media

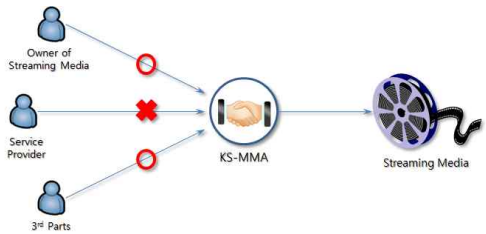

그림 15. 제안된 KS-MMA에 의한 스트리밍 미디어의 접근 제어
Fig. 15. Access control of streaming media by proposed KS-MMA

StraaS 데이터 센터에 분산되어 저장된 암호화된 스트리밍 미디어는 컨테이너로 통합 및 복호화되어야 한다. 암호화된 스트리밍 미디어의 복호는 다자간 매칭 인증에 의한 키 생성에 의해서 복호화가 되며, 그림 15와 같은 기능을 수행하게 된다. 다자간 매칭 인증은 사용자들 중에서 임의의 사용자 이상의 합의가 이루어져야 스트리밍 미디어가 복호화를 위한 키가 생성되며, 그림 16과 같이 나타낸다.

다자간 정합 인증 시스템은 모든 합의된 사용자 중에서 과반수 이하가 합의하지 않더라도 KS-MMA에 의해서 역할의 위임 받고, 복호화 및 접근 제어를 위한 키를 생성하게 된다. 시스템을 운용을 위해서는 사용자 인증이 필요하며, 사용자에게는 아이디와 아이디에 해당하는 업무의 역할을 할당하게 된다. 또한 할당된 아이디는 상위 역할을 위임하기 위한 인증 절차로 다자간 정합을 이용한다. 하위의 역할자 n명중에서 50%이상이 합의를 하면 그림 1에서와 같이 3명중에서 2명만 합의하면 상위 담당자의 역할을 위임할 수 있게 인증을 제공한다. 상위의 담당자가 부재시에, 50%이상에 해당하는 ID2와 ID3에 합의에 의해서 ID2의 B와 C부분, ID3의 A와 C부분의 결합으로 상위 담당자의 역할을 인증하게 된다. 또한 ID2와 ID3은 C부분에 의해서 서로가 같은 등급임을 파악 및 위조에 대응하게 된다.

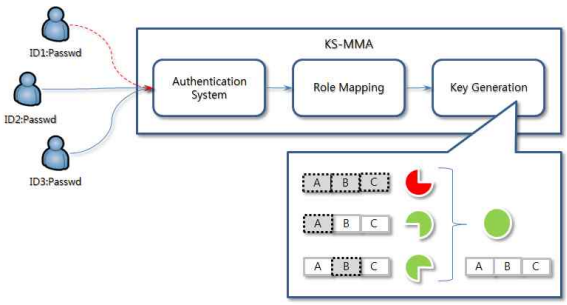

그림 16. KS-MMA에 의한 키 생성 과정의 개념도
Fig. 16. Concept diagram of key generation process by KS-MMA

4-3 검색 가능 이미지 암호 시스템 (SIES)

검색 가능 암호 시스템은 암호화된 자료를 복호화하지 않고도 원하는 자료를 검색할 수 있는 암호 기반 기술이라면 검색 대상을 텍스트에서 이미지로 확장하여 검색 가능 이미지 암호 시스템 (SIES; Searchable Image Encryption System)을 설계한다. 검색 가능 암호 시스템은 개인의 정보가 외부 저장 공간에 저장되면서 발생하는 프라이버시 등의 여러 문제점에 대한 해결 방법으로 지금까지 많은 연구가 진행되었으나, 본 연구에서는 이미지로 확장하여 StraaS에서 검색 가능 이미지 암호 서비스를 제공한다. SES(Searchable Image Encryption System)에서 정보를 포함하는 문서와 키워드를 이용해서 숨기고 싶은 정보를 암호화하고, 사용자가 자신이 원하는 암호화된 문서를 검색하기 위해 서버에 제공하는 정보를 키워드를 이용하여 검색한다. 제안하는 SIES에서는 문서를 스트리밍 미디어로, 문서에 포함된 키워드는

스트리밍 미디어의 여러 이미지들로 확장한다. 즉, SES의 수식 (1)을 수식 (2)로 확장하여 정의한다.

$$Streaming\,Media = \{ IMG_1, IMG_2, \cdots, IMG_n \} \quad (2)$$

SIES는 SES와 동일하게 키 생성(key generation), 암호화(build index), 트랩도어 생성(trapdoor generation), 검색(search)의 4가지 단계로 이루어지며, 키 생성 단계에서 약간의 전처리(Pre-processing)가 추가된다. 키 생성 단계에서 사용자가 앞으로 사용할 검색 가능 이미지 암호 시스템을 준비하는 단계이며, 이 부분이 KS-MMA가 키 생성 단계를 대처하게 된다.

V. StraaS의 응용 모델

제안하는 StraaS 서비스를 이용한 응용 영역들과 비즈니스 모델을 제안하며, 이에 한정되지는 않는다.

5-1 기존 서비스에 확장 기능 부여

EBS 방송은 교육을 위한 스트리밍 서비스를 제공하고 있으며, PC 및 일부 테블릿 기반의 몇몇 스트리밍 미디어 포맷을 지원하고 있다. 간략하게, EBS 사이트에서 제공하는 디지털 콘텐츠의 활용을 증대시키고, 디지털 미디어 소비를 위한 확장 기능을 제공할 수 있다. 예를 들면, 애플의 iPad2에서 스트리밍 서비스를 이용하기 위해서는 EBS 사이트에서 미디어를 PC로 다운로드 후에 iPad2에서 재생 가능한 미디어 포맷으로 변환한다. 그리고 변환된 미디어를 iTune을 이용해서 iPad2로 전송하여야 한다. 이러한 복잡한 절차를 StraaS를 이용하여 단축시킬 수 있으며, 스트리밍 미디어의 소비를 위한 다양한 변환을 온토롤지를 이용하여 단말 장치인 PC, 모바일 및 테블릿, 핸드폰 등에 최적화된 미디어 변환을 준 실시간으로 가능하다.

5-2 StraaS의 인프라 통합 기능

StraaS의 인프라 통합 기능은 한 영역에 분포된 이미지 또는 영상을 캡쳐할 수 있는 장치들에서 생성되는 미디어를 통합하여 임의의 개체에 대한 스토리에 해당하는 스트리밍 미디어의 생성할 수 있다. 그림 17은 스트리밍 미디어의 메타 정보를 이용하는 개념도이며, 그림 18은 이러한 개념의 응용 예를 나타낸 것이다.

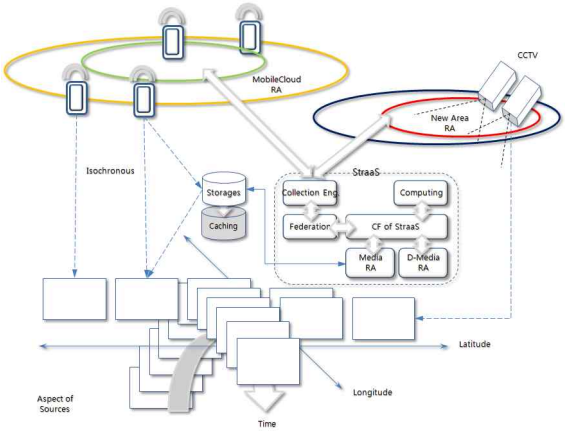

그림 17. 시간 및 위치 정보의 메타 정보를 이용한 서비스 제공
Fig. 17. Service support using meta information of time and location data

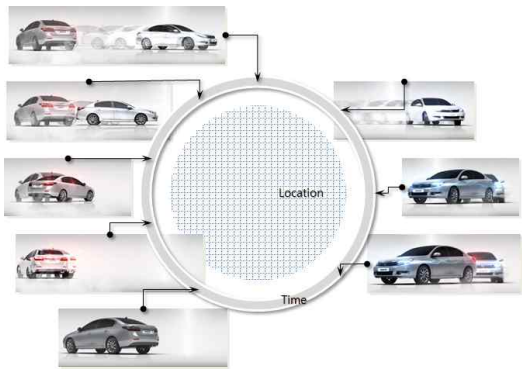

그림 18. StraaS의 메타 정보에 의한 새로운 응용 서비스 지원
Fig. 18. New application service support by meta information of StraaS

VI. 결 론

본 논문은 클라우드 기반의 스트리밍 서비스와 보안을 제공하는 StraaS 서비스를 설계하였다. 클라우드 컴퓨팅 기반의 스트리밍 서비스를 제공하기 위한

Streaming as a Service(StraaS)를 정의하며, StraaS 서비스를 제공하기 위한 다양한 기능과 보안 기능에 대해서 기술하였다. 특히 클라우드 컴퓨팅과 스트리밍 서비스를 위한 보안 기능으로 KS-MMA는 다자간 정합 인증에 의한 접근 제어를 제공하며, SIES는 스트리밍 미디어의 프라이버시를 제공할 수 있다.

참 고 문 헌

[1] McKinsey, "Big Data: The next frontier for innovation, competition, and productivity", May 2011.

[2] 가드너 그룹, http://www.gartner.com

[3] P. Golle, J. Staddon, and B. Waters, "Secure Conjunctive Keyword Search over Encrypted Data," *In Applied Cryptography and Network Security Conference 2004,* June 2004.

[4] B. Waters, D. Balfanz, G. Durfee, and D. Smetters, "Building an Encrypted and Searchable Auditlog," *NDSS 2004,* Feb. 2004.

[5] R. Ostrovsky and W. Skeith, "Private Searching on Streaming Data," *Crypto 2005*, August 2005.

[6] J. Bethencourt, H. Chan, A. Perrig, E. Shi, and D. Song, "Anonymous Multi-Attribute Encryption with Range Query Conditional Decryption," *Technical Report, C.M.U.*, 2006.

[7] 조남수, 홍도원, "검색 가능 암호 시스템 기술 동향," *전자통신동향분석 제23권 제4호* 2008년 8월.

[8] GStreamer, http://www.gstreamer.net

[9] OpenStack, http://www.openstack.org

차 병 래 (車炳來)

2004년 2월 : 국립 목포대학교 컴퓨터공학과(공학박사)
2005년 3월 ~ 2009년 2월 : 호남대학교 컴퓨터공학과 전임강사
2009년 9월~현재 : 광주과학기술원 (GIST), 정보통신공학부 연구교수

관심분야 : 정보보안, Intrusion Detection System, 신경망, 클라우드 컴퓨팅, Future Internet 등

심 수 정 (沈守正)

1996.2월 호남대학교 컴퓨터공학과 학사(졸)
1999.2월 전남대학교 전산학과 석사 (소프트웨어공학)
2003.8월 전남대학교 전산학과 박사 과정 수료(자연어처리)
2012.3 호남대학교 초빙교수

관심분야: 자연어 처리, 문서분류, 정보검색 등

김 용 일 (金容日)

1984년 3월 : 전남대학교 계산통계학과 (이학사)
1986년 2월 : 한국과학기술원 전산학과 (공학석사)
1986년 3월~1994년 2월 : 한국원자력 연구소 선임연구원
1994년 3월~2000년 2월 : 초당대학교 컴퓨터학과 조교수
2002년 3월~현재 : 호남대학교 인터넷콘텐츠학과 조교수

관심분야 : 지능형정보검색, 클라우드 컴퓨팅, 지능형 에이전트 등