情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

클라우드 컴퓨팅을 활용한 D-CATV의 사용자 인증 및 접근 제어 방법연구

양 종 원*, 이 상 동*, 채 종 수**, 서 창 호***

요 약

기존의 케이블 방송망을 활용하여 개인화 방송 서비스를 제공하기 위해서는 하드디스크 등 PC형태를 갖춘 고가의 셋톱 박스가 필요하며, SO 별로 서비스 제공을 위한 독립적인 인프라 구축이 필요한 실정이다.

D-CATV 사업자의 경우 고화질 디지털 방송을 앞세워 한시적인 주문형 비디오 서비스 및 한정적인 웹서비스와 유사한 형태의 부가서비스를 제공하고 있으나, 기존 TV의 영역을 넘어선 IP망의 특성을 활용한 양방향서비스, 개인화 서비스를 원활히 제공하지 못하고 있다. 이는 IPTV 사업자와 치열한 경쟁에서 서비스 측면에서 지속적인 열세의 빌미가 될 것이다.

본 논문에서는 스토리지 클라우드 컴퓨팅 환경을 적용한 차세대 D-CATV 서비스를 위해 SO업체들이 공동활용 가능한 클라우드 인프라 구축과 양방향 개인화 서비스 등 차세대 디지털방송 기반 기술을 위한 HDFS 기반 가상화된 스토리지 클라우드 시스템을 제안하며, 또한 D-CATV 서비스 접속을 위한 사용자 인증 및 콘텐츠 접근제어 시나리오 방법을 제안하였다.

Ⅰ. 서 론

공중파, IPTV, DMB, 위성방송 등 방송 서비스의 형태가 다변화 되면서 방송 산업내부의 경쟁이 심화되고 있으며, 이러한 경쟁에서 우위를 차지하기 위해 개인화 된 고급서비스(UCC, CUG 방송, VOD, PVR)이 각광을 받고 있다. 특히 IPTV 사업자의 경우 고화질의 콘텐츠 서비스를 제공, 풀 브라우징 도입, 검색서비스, 쇼핑 서비스 등 새로운 방송/통신 융합에 매우 활발하게 진행하고 있다.

하지만 국내 케이블 방송 사업자는 기술적 기반이 취약하여 개인화 방송 서비스, 양방향 방송 서비스 등을 도입하는데 있어 한계를 느끼고 있으며, 사업자간 표준 제정, 인프라 공통 활용 기반이 약해 인프라 투자에 대한 부담을 느끼고 있는 상황이다.

본 논문에서는 스토리지 클라우드 컴퓨팅 환경을 적용한 차세대 D-CATV 서비스 시스템을 제안한다. 제안된 시스템은 스토리지와 서비스 서버간의 병목을 해소하기 위하여 서비스 빈도가 높은 콘텐츠를 캐시 서버에 유지하고, 부하분산 서버가 관리하는 형태로 설계하였다.

또한, 차세대 D-CATV의 안전한 사용자 인증 서비스를 위해 SAML을 이용한 사용자 인증 기술, 콘텐츠 접근제어 기술을 적용하였다.

Ⅱ. 관련연구

2.1 D-CATV

D-CATV(Digital Cable Television)는 기존의 아날로그 CATV를 디지털 기술로 업그레이드한 방송이다.

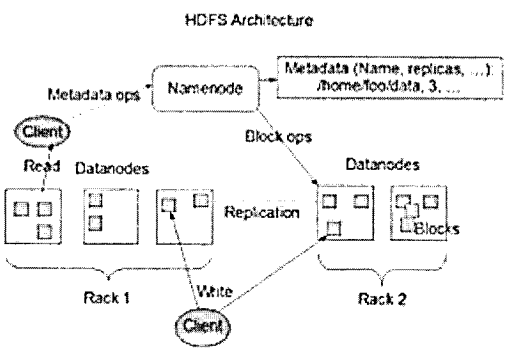
* 한국과학기술정보연구원 슈퍼컴퓨팅본부 (jwyang,sdlee@kisti.re.kr)
** 공주대학교 일반대학원 군사정보학과(정보보호전공) 박사과정 (jsc0230@hanmail.net)
*** 공주대학교 일반대학원 응용수학과 정교수 및 군사정보과학 부교수(chseo@kongju.ac.kr)

D-CATV는 HD(High Definition)급 고화질 방송과 고음질 서비스를 비롯해 아날로그 방송에서는 불가능했던 쌍방향 서비스까지 제공할 수 있어 차원이 다른 서비스로 인정받고 있다.

한국의 D-CATV는 HFC(Hybrid Fiber-Coaxial)의 특성을 가지고 있다. 국내 SO(System Operator)들은 이미 디지털 방송이 가능한 수준인 750MHz 급의 HFC 네트워크를 갖추고 있다. 이 중에서 현재 60~70개 가량의 아날로그 채널이 450MHz 정도를 차지하고 있고, 디지털 방송이 나머지 주파수를 사용할 수 있다. 한 개의 HD급 채널을 방송하기 위해 6MHz에 해당하는 주파수가 필요한 것을 감안하면, 50개 가량의 디지털 채널을 추가로 제공할 수 있게 되는 것이다. 아날로그 방송이 중단되는 2010년경에는 450MHz 이하 주파수까지도 디지털 방송용으로 사용할 수가 있어 디지털 채널 수는 HD급 방송으로만 약 120개까지 늘어날 전망이다. 더욱이 HD급으로 제공될 수 있는 콘텐츠가 제한되어 있다는 점과 HD급 이하인 SD(Standard Definition)급 채널이 HD급보다 약 1/3, 1/4 정도의 주파수만 필요로 한다는 점을 감안하면 디지털 방송 채널 수는 더욱 늘어날 것으로 보인다.

2.2 HDFS

HDFS[3]는 Mater/Slave 구조를 가지고 있다. HDFS 클러스터는 파일 시스템 네임스페이스를 관리하고 클라이언트에 의한 파일 접근을 통제하는 마스터 서버의 단일 NameNode로 구성된다. 추가적으로 클러스터에서 노드당 하나며 노드에 붙은 스토리지를 관리하는 수 많은 Datanodes가 있다. HDFS는 파일 시스템 네임스페이스를 노출하고 사용자의 데이터를 파일로 저장되도록 허용한다. 내부적으로 파일은 하나 또는 그 이상의 블럭으로 쪼개지며 이러한 블럭들은 Datanodes의 집합 안에 저장된다.



〔그림 1〕 HDFS Architecture에서 NameNode와 Datanodes

NameNode는 파일과 디렉터리의 열기, 닫기, 이름 변경과 같은 파일 시스템 네임스페이스 동작을 수행한다. 또한 Datanodes로의 파일 블럭의 매핑을 판단한다. Datanodes는 파일 시스템의 클라이언트들로부터의 읽기와 쓰기 요청을 제공하는 역할을 하며, NameNode의 지시에 따라 블록 생성, 삭제 그리고 복제를 수행한다.

2.3 클라우드 컴퓨팅 보안 이슈

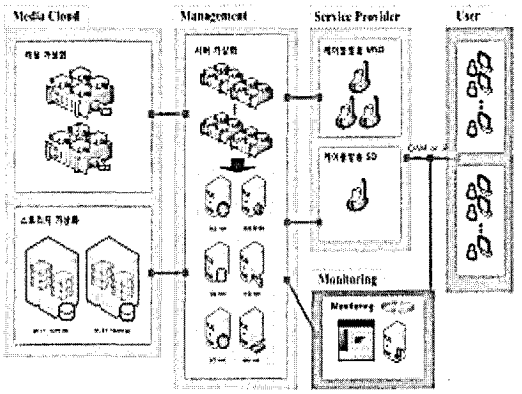
클라우드 컴퓨팅의 보안요소는 기존에 발표된 가트너 보고서[4]의 7가지 클라우드 컴퓨팅의 기술적 그리고 비즈니스 위험요소, UC Berkeley 10가지 기획요소[5] 그리고 CSA[6]의 14가지 클라우드 컴퓨팅 보안 요소를 모두 검토하여 보면, 이들 보고서들의 내용은 기존의 보안 위협과 클라우드 컴퓨팅 환경으로 인한 기술적, 비즈니스 관련 위협요소를 잘 나타내고 있다.

기술적, 관리적, 물리적 관점의 클라우드 컴퓨팅 보안 기술을 고려할 때, 먼저 기술적 보안 기술로 암호, 키 관리, 네트워크 보안, 인증(SSO, SAML, Kerberos), IAM(Identity Authentication Management), 방화벽,접근제어, ACL, DB보안, 시스템보안, Log Auditing, Secure VM, Secure Hadoop 등을 생각할 수 있으며, 관리적 기술로 컴플라이언스, SLA(Service Level Agreement), 로깅, 모니터링, 감사 등이며, 물리적 보안 기술로 BC, 백업, 재난복구, 출입통제 등이 예상된다.

Ⅲ. 제안 시스템

3.1 Single-Site 스토리지 시스템 제안

Single-site 스토리지 시스템은 차세대 D-CATV 제공하기 위한 기본 서비스 인프라이다. 클라우드 컴퓨팅 환경을 적용하기 위해서는 콘텐츠에 대한 동기화/분배하는 기술과 콘텐츠를 효율적으로 저장/관리하는 분산 파일 시스템이 요구된다. 또한 사용자 요구에 따른 콘텐츠 제공에 있어서 스토리지와 QoS 보장을 위한 모니터링 시스템이 필요하다. 아래 [그림 2]은 single-site 스토리지 시스템의 구성요소와 방송 서비스를 위한 인프라를 보여준다.



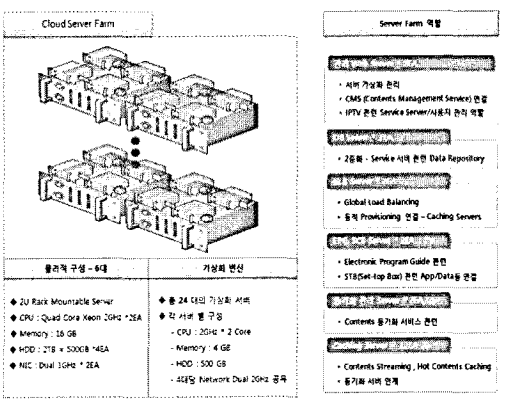
〔그림 2〕 Single-Site 스토리지 시스템 구성도

세부적으로 필요 구성요소를 크게 서버 가상화, 캐싱 가상화, 스토리지 가상화로 구별하였다.

○ 서버 가상화

디지털 케이블 방송서비스를 제공하기 위해서는 관리적인 측면에서 여러 가지 서버들이 요구된다. 자원의 효율적인 운용과 비용절감이 최대 장점인 클라우드 컴퓨팅을 적용하여 물리적인 6대의 서버를 이용하여 24대의 가상화 서버를 운용한다.

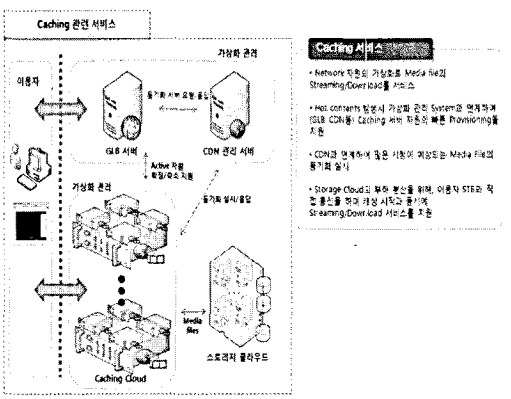
관리 Web 서버는 가상화 서버들을 관리하며, 사용자에게 콘텐츠를 제공하기 위해서 CMS(Contents Management Service)와 연결하여 해당 서비스를 제공한다. GLB 서버는 Global Load Balancing을 제공하기 위한 서버로써 캐싱 서버와 연결되어 사용량이 많은 콘텐츠에 대한 동적 프로비져닝을 제공한다. EPG, SCS 서버는 디지털 케이블 방송의 프로그램에 대한 Electronic Program Guide와 사용자의 STB 관련 APP/Data 등을 관리한다. 캐싱 서버와 동기화 관리 서비는 요구량이 많은 콘텐츠에 대한 캐싱 서비스와 동기화 서비스를 제공한다.



〔그림 3〕 서버 가상화 구성

○ 캐싱 가상화

사용자의 콘텐츠 요구나 스토리지 시스템의 부하를 최소화하기 위해서는 해당 방송서비스를 위한 캐싱 서버가 필요하다. 캐싱 서버는 사용량이 많은 콘텐츠를 저장하고 있어 사용자들에게 고품질의 서비스를 가능하게 할 뿐 아니라 양방향 서비스를 위한 업로드를 위한 저장 공간도 가지고 있다.



〔그림 4〕 캐싱 서비스

사용량이 많은 콘텐츠를 GLB 서버에서 파악하여 해당 콘텐츠를 동기화 솔루션을 이용하여 여러 동기화 서버에 보유하게 되며, 네트워크 부하를 최소화 가능하게 한다. 캐싱 서비스 관련하여 다음과 같은 서비스가 가능하다.

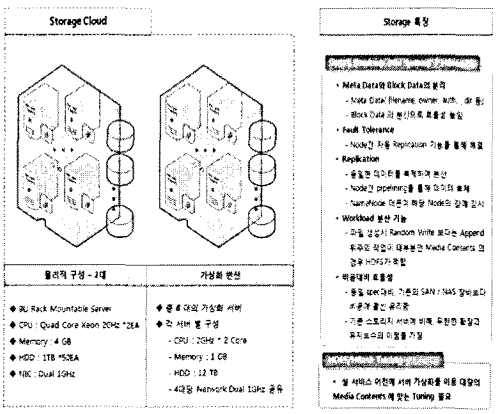
- 네트워크 자원을 가상화하여 콘텐츠 파일을 스트리밍/다운로드 서비스
- Hot 콘텐츠에 대한 가상화 관리 서버(GLB, CDN)와 연계한 동적 프로비저닝
- CDN과 연계하여 많은 시청이 예상되는 콘텐츠 파일에 대한 동기화
- 스토리지 클라우드 부하 분산을 위한 사용자 STB와 직접 통신/캐싱서비스

캐싱 서비스를 위해서는 GLB 서버와 CDN 관리 서

버의 효율적인 운용이 필수적이며, 사용자 요구량에 따른 콘텐츠 동기화 및 캐싱 서비스를 동적으로 제공하는 것이 필요하다.

○ 스토리지 가상화

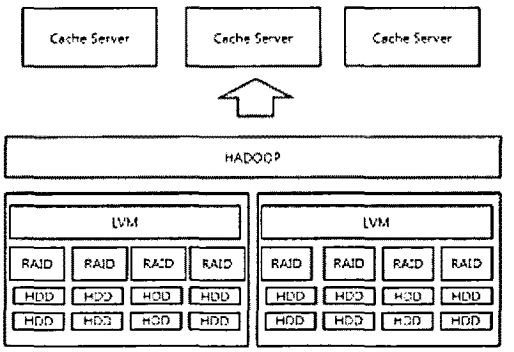
클라우드 컴퓨팅에서 스토리지 가상화는 물리적으로 서로 다른 여러 스토리지 컨트롤러에 분포되어 있는 유휴 시스템 자원(디스크)을 모아서 하나의 논리적은 가상 디스크 자원으로 제공해 주는 기술이다. 디지털 케이블 방송서비스에 사용되는 콘텐츠는 대용량 파일이 대부분이며, 이를 위한 대규모 스토리지의 구성은 확장성이 필수적이다.



〔그림 5〕 스토리지 가상화 구조도

디지털 케이블 방송서비스에 스토리지 클라우드를 적용하기 위해서는 적합한 파일시스템을 선택하여야 한다. 방송서비스가 콘텐츠의 생성이 나날이 늘어남에 따라 스토리지의 확장성이 용이하며, 콘텐츠 파일에 대한 대용량 처리의 빈번히 발생과 관련하여 전송률이 높은 파일시스템이 요구된다. Hadoop 파일 시스템은 이러한 요구조건 및 결함인내형, Replication, 워크로드 분산등 여러 장점이 있다. 또한 동일 스펙 대비 기존 SAN/NAS 장비보다 비용적인 측면에서 강점을 보인다.

본 논문에서 제안한 시스템은 대용량 스토리지는 POP서버에 미디어 파일을 전송하는 Cache 서버와 통신하여 원하는 동영상을 스트리밍 서비스할 수 있도록 해 주어야 한다. 즉, 대용량 스토리지의 외부 인터페이스에 Cache 서버와 통신할 수 있는 방법이 있어야 하는데, 대용량 스토리지를 관리하는 Hadoop은 위에서 언급한 다양한 형태의 인터페이스를 제공한다. 이 인터페이스를 이용해서 Cache 서버들은 Hadoop이 block단위로 저장하고 있는 컨텐츠 내용에 접근할 수 있다 [그림 6].



〔그림 6〕 스토리지 인터페이스

다수의 HDD를 RAID로 묶어 대용량 device을 만들고, LVM을 구성한 후, Hadoop을 이용한 이런 구현의 장점은 용량의 확장이 용이하고, Hadoop의 복제 기능을 이용해서 분산 서버들의 전체 시스템 차원에서의 이중화 기능을 수월하게 구현할 수 있다는 점이다.

3.2 HDFS Storage Cloud

호스트 미디어 파일 및 STB에 관련된 파일들의 개수와 사이즈는 수 Peta의 대단위 대용량 사이즈로 예측이 된다. 기존의 NAS, SAN등의 장비로는 비용 및 물리적인 한계가 있으며, 이를 해결하기 위해 최근에 이슈가 되고 있는 HDFS을 활용 및 재가공하여 가상화된 스토로지 클라우드 시스템을 설계하였다.

HDFS은 일반적인 하드웨어에서 실행할 수 있도록 디자인된 분산 파일 시스템으로 fault-tolerant하고 저비용 하드웨어를 통해 배포할 수 있도록 설계되었으며, 응용프로그램 데이터의 접근에 높은 처리량을 제공하고, 대용량 데이터 집합을 갖는 응용 프로그램에 적합하다는 특징이 있다.

본 논문에서는 HDFS 기반 스토리지 클라우드 구축에 있어서 주요 가정과 목표는 다음과 같이 정의 하였다.

○ **Hardware Failure**

Hardware Failure는 Exception과는 뚜렷하게 다른

기준이다. HDFS 인스턴스는 파일 시스템의 데이터의 부분을 저장하는 서버 장비의 수백 또는 수천으로 구성될 수 있으며, 이러한 대단히 많은 구성요소는 불분명한 실패의 확률을 갖는다. 즉, HDFS의 일부 구성요소는 항상 기능을 수행하지 못한다고 가정해야 하며, 따라서 결함의 탐지와 빠르고 자동적인 복구는 HDFS의 핵심적인 구조적 목표이다.

○ **Streaming Data Access**

HDFS에서 수행되는 응용 프로그램은 그들의 데이터 결합을 위하여 스트리밍 접근을 필요로 한다. HDFS는 사용자에 의한 상호작용적(interactive) 사용 대신 배치 프로세싱에 더 적합하게 설계되었으며, 강점은 데이터 접근의 낮은 지연(low latency)보다는 빠른 데이터 accessing이라고 할 수 있다. HDFS는 POSIX의 몇 가지 불필요한 사항들을 데이터 처리율의 향상으로 대체하였다.

○ **Large Data Sets**

HDFS에서 수행되는 응용 프로그램은 대용량 데이터 집합을 가진다. HDFS에서의 일반적인 파일은 기가 바이트부터 테라 바이트의 용량이라고 생각되며, 대용량 파일들을 지원할 수 있도록 튜닝되었다. 그것은 데이터 처리의 높은 대역폭과 단일 클러스터에서의 수백 노드로의 확장을 제공해야 한다. 또한 단일 인스턴스에서 수천만 파일을 제공해야 한다.

○ **Simple Coherency Model**

HDFS 응용 프로그램은 파일에 대해 한번 쓰고 여러 번 읽는(write-once-read-many) 접근 모델을 필요로 한다. 파일이 한번 생성되고, 쓰여지고, 닫히면 변화를 필요로 하지 않는다. 이런 가정은 데이터 간섭 이슈를 단순화하고 높은 처리량의 데이터 접근을 가능하게 한다. MapReduce 응용 프로그램, 웹 크롤러 응용 프로그램, 대단위 미디어 파일 처리 프로그램 등은 이 모델에 완벽하게 적합하다. 또한, 추후에는 파일에 추가-쓰기(appending-writes)를 제공할 계획이 있어야 한다.

○ **Moving Computation is Cheaper than Moving Data**

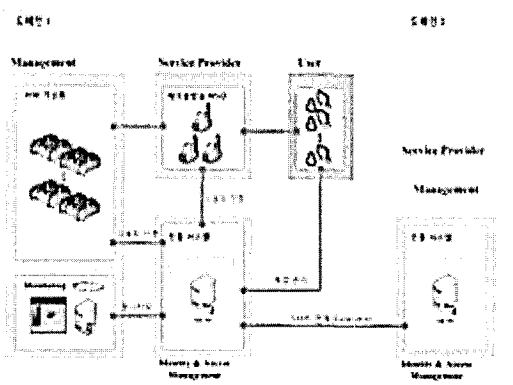
응용 프로그램에 의해 요청된 계산은 만약 그것이 수행하는 데이터 근처에서 실행된다면 보다 더 효율이다. 이것은 데이터 집합의 사이즈가 대단히 클 때 특히 사실입니다. 이것은 네트워크 트래픽을 최소화 시키고 시스템의 전체적 처리량을 증가시킨다. 가정은 응용 프로그램이 수행 되는 곳으로 데이터를 옮기는 것 보다 데이터 가까이로 계산을 옮기는 것이 더 낫다는 것이다. HDFS는 데이터가 위치한 곳 가까이로 그들을 옮길 수 잇도록 응용 프로그램을 위한 인터페이스를 제공한다.

○ **Portability Across Heterogeneous Hardware and Software Platforms**

HDFS는 한 플랫폼에서 다른 플랫폼으로 쉽게 이식할 수 있도록 디자인되었다. 이것은 응용 프로그램의 대형 집합을 위한 선택의 플랫폼으로써 HDFS의 광범위한 적용을 용이하게 했다.

3.3 제안된 사용자 인증 및 접근제어 보안

본 논문에서 Single-Site 스토리지 시스템을 제안하면서 사용자 인증 및 접근제어에 대한 보안 기술을 요구하게 되었다. CSA 권고 사항 중 사용자 계정 및 접근에 대한 보안적인 이슈사항을 검토하여 클라우드 컴퓨팅 환경에서의 보다 안전한 D-CATV 서비스 시스템을 하기 위해서는 먼저 SAML 기반의 SSO(Single Sign On) 지원을 통한 서로 다른 도메인간의 인증 기반 기술이 필요하다. SAML을 기반으로 하는 SSO을 구축하는 경우 일반적인 SSO 시스템을 구축하는 것에 비해 탁월한 호환성을 가지게 됨으로 인해 다양한 벤더간의 사용자 인증이 안전하게 수행될 수 있으므로, 본 시스템에서는 SAML 기반의 SSO가 필수적이다.

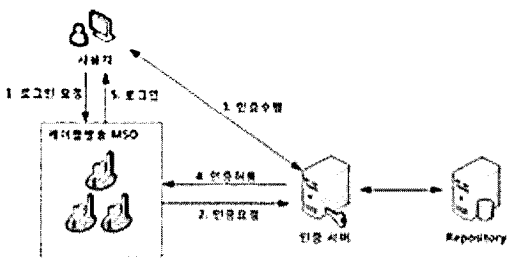


〔그림 7〕 인증시스템 서비스 구성

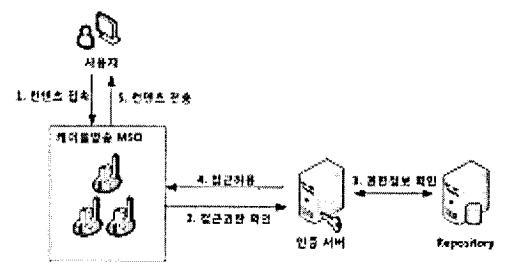
제안된 시스템에서는 SAML Push 모델을 기반을 두고 있으며, 다음과 같은 인증시스템 서비스 구성을 가진다.

사용자 계정 통합 관리를 위해 가상화 시스템에 대한 사용자 계정 정보를 통합관리를 하며, SP(Service Provider)와 연계된 사용자 계정 정보를 공유한다. 또한 SAML을 기반으로 하는 사용자 계정정보의 공유 및 연계를 하며, 인증된 사용자의 모니터링 및 사용자의 콘텐츠 접근에 대한 모니터링을 수행한다.

세부 서비스 시나리오는 다음과 같다.



〔그림8〕 사용자 인증 처리



〔그림 9〕 콘텐츠에 대한 접근 처리

Ⅳ. 결 론

본 논문에서는 스토리지 클라우드 컴퓨팅 환경을 적용한 차세대 D-CATV 서비스 시스템을 보였으며, 또한, 차세대 D-CATV의 안전한 사용자 인증 서비스를 위해 SAML을 이용한 사용자 인증 기술 및 콘텐츠 접근제어 기술을 제안하였다.

향 후, 케이블 방송망 기반 다수의 SO가 공동활용 가능한 클라우드 인프라 구축을 통해 양방향 개인화 서비스 등 차세대 디지털방송 기반 기술 개발 및 표준을 도출하고 이기종 저가 STB 활용 가능한 범용적인 미들웨어를 구축할 것이다.

참고문헌

[1] D.R. Aadsen. H. N. Scholz. and Y. Zorian. Automated BIST for Regular Strategies Em-bedd in ASIC Devices. AT&T Technical Journal. May/June. 1990.

[2] 3GGP2 C.S0001. "cdma2000 - Introduction".

[3] 3GGP2 C.S0002. "physical Layer Standard for cdma2000 Spread Spectrum Systems".

[4] 3GGP2 C.S0003. "Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum Systems".

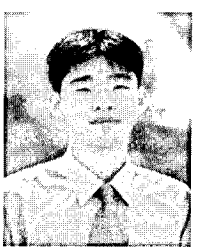
[5] 3GGP2 C.S0004. "Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems".

[6] H. Fathallag, L. A. Rusch and S. LaRochelle, "Passive optical fast frequency-hop CDMA communications system," IEEE J. of Lightwave Tech, Vol. 17, No. 3, 1999.

[7] Frank Quick. "Security in cdma2000". ITU-T Workshop on Security. Seoul(Korea). 13-14 May. 2002.

[8] R. J. Francis, J. Rose and Z. Vranesic, "Chortle-crf : Fast Technology Mapping for Lookup Table-based FPGAs," 28th DAC, 1991.

〈著者紹介〉



양 종 원 (Jong Won Yang)
정회원
2009년: 공주대학교 바이오정보학과 (정보보호전공) 박사졸업
2006년~2008년: 한국전자통신연구원 위촉연구원
2009년 7월~현재: 한국과학기술정보연구원 선임연구원
<관심분야> 클라우드 컴퓨팅보안, HPC 시스템 보안, 암호알고리즘 등

이 상 동 (Sang Dong Lee)

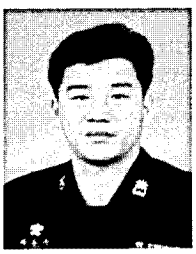
정회원

2000년: 부산대 물리학과(이론물리학전공) 박사 졸업

2000년 ~ 2002년 Senior Researcher, Safeweb.com Inc., Emeryville, CA, US

2003년 3월 ~ 현재 : 한국과학기술정보연구원 책임연구원

<관심분야> 클라우드 컴퓨팅, e-Science



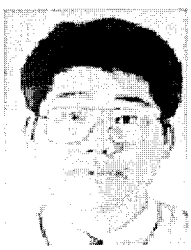
채 종 수 (Jong Soo Chae)

정회원

2003년: 전남대학교 컴퓨터공학 석사

2008년 ~ 공주대학교 군사정보과학 (정보보호전공) 박사과정

<관심분야> NCW, C4I, 국방인터라넷, 정보보호, 무선암호 등



서 창 호 (Chang Ho Seo)

1992년: 고려대학교 일반대학원 수학과 (이학석사)

1996년: 고려대학교 일반대학원 수학과 (이학박사)

1996년~1996년: 국방과학연구소 선임연구원

1996년~2000년: 한국전자통신연구원 선임연구원, 팀장

2000년~현재: 공주대학교 응용수학과(정보보호전공) 정교수

2001년~현재: 공주대학교 바이오정보학과 부교수 및 군사정보과학 부교수

<관심분야> 암호 알고리즘, PKI, 무선 인터넷 보호 등