Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 9 pp. 12-20, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.9.12
ISSN 1975-4701 / eISSN 2288-4688

클라우드 환경에서 안전한 스토리지 접근 제어를 위한 권한 관리 프로토콜 설계

민소연[1], 이광형[2*], 진병욱[3]
[1]서일대학교 정보통신과, [2]서일대학교 인터넷정보과, [3]숭실대학교 컴퓨터학과

A Design of Authority Management Protocol for Secure Storage Access Control in Cloud Environment

So-Yeon Min[1], Kwang-Hyong Lee[2*], Byung-Wook Jin[3]
[1]Dept. of Information and Communication, Seoil University
[2]Dept. of Internet Information, Seoil University
[3]Dep. of Computer Science, Soongsil University

요 약 기존의 주력산업의 고도화 및 고부가가치 산업이 창출되고 있는 가운데 클라우드 컴퓨팅 기반의 융합서비스가 등장하였다. 사용자 개인의 밀착서비스부터 산업용 서비스까지 다양한 융합서비스가 제공되고 있으며 국내에서는 클라우드 서비스 기반의 금융, 모바일, 소셜 컴퓨팅, 홈서비스를 중심으로 경제 전반에 걸쳐 기존 산업시장의 원동력이 되고 있다. 그러나 클라우드 스토리지 환경에서 Dos, DDos공격뿐만 아니라 스토리지 서버의 중요 데이터를 타깃으로 한 공격기법들이 발생하고 있으며, APT, 백도어 침투, 특정 대상에 대한 다단계 공격과 같은 감지하기 어려운 보안위협들이 발생하고 있다. 이를 보완하기 위해서 본 논문에서는 사용자들로 하여금 안전한 스토리지 서비스를 제공하는 권한 관리 프로토콜에 관하여 설계하였으며, 클라우드 환경과 빅데이터 기반 기술의 융합사례와 보안위협 및 요구사항에 대해서 연구하였고, 클라우드 컴퓨팅 환경과 빅 데이터 기술의 융합사례와 보안위협 및 보안 요구사항에 대해서 관련연구를 수행하였다. 이를 기반으로 제안된 프로토콜은 기존의 클라우드 환경과 빅데이터 기반 기술에서 발생하는 공격기법에 대해서 안전성을 분석하였고, 세션키 생성부분에서 대략 55%의 향상성을 확인 할 수 있었다.

Abstract With the enhancements in existing major industries, cloud computing-based converging services have been created, as well as value-added industries. A variety of converging services are now provided, from personalized services up to industrial services. In Korea, they have become the driving force behind existing industries throughout the whole economy, but mainly in finance, mobile systems, social computing, and home services, based on cloud services. However, not only denial of service (DOS) and distributed DOS (DDOS) attacks have occurred, but also attack techniques targeting core data in storage servers. Even security threats that are hardly detected, such as multiple attacks on a certain target, APT, and backdoor penetration have also occurred. To supplement defenses against these, in this article, a protocol for authority management is designed to provide users with safe storage services. This protocol was studied in cases of integration between a cloud environment and big data-based technology, security threats, and their requirements. Also studied were amalgamation examples and their requirements in technology-based cloud environments and big data. With the protocol suggested, based on this, security was analyzed for attack techniques that occur in the existing cloud environment, as well as big data-based techniques, in order to find improvements in session key development of approximately 55%.

Keywords : Access Control, Authority Management, Cloud Computing Storage Service, Management Protocol, Message Communication

*Corresponding Author : Kwang-Hyong Lee(Seoil Univ.)
Tel: +82-2-490-7226 email: dreamace@seoil.ac.kr
Received August 26, 2016 Revised September 8, 2016
Accepted September 9, 2016 Published September 30, 2016

1. 서론

최근의 IT 기술의 패러다임은 클라우드 환경으로 전환하고 있으며, 국내외 기관 및 기업은 클라우드 개발 생태계를 조성하기 위해 기술들을 연구하고 있다[1,8-11]. 클라우드 플랫폼 서비스에 대해서 연구 및 기술을 개발하여 사용자들로부터 편의성 높은 서비스를 제공하고 있다. 그리고 금융, 의료, 자동차, 농•수산업 분야와 같은 다른 산업과 결합하고 빅 데이터와 인공지능 등 ICT분야의 신기술과 융합하여 보다 다양한 다양한 서비스를 제공할 수 있는 장점이 있다[2].

클라우드 서비스는 사용자로 하여금 다양한 서비스와 편리한 서비스를 제공하고 있지만, 해커로부터의 첫 번째 타깃이 될 수 있다. 과거의 스토리지 서비스를 공격할 때는 APT를 활용한 공격이 대다수였던 반면, PC보다 허술한 스마트 폰, 태블릿 PC와 같은 모바일 기기를 활용하여 내부정보를 유출하는 사례가 발생하고 있다[1-3,8]. 또한 ICT기반의 기술이 활성화되면서 기밀 정보유출 뿐만 아니라 금전, 생명을 위협하는 공격기법을 사용함으로써 클라우드 서비스를 이용하는 사용자들로부터 신뢰감을 떨어뜨릴 수 있다[3]. 본 논문에서는 클라우드 환경의 스토리지 서비스에 접근제어와 권한 관리 프로토콜에 대해서 연구하도록 한다. 제안된 논문은 등록과정을 수행하여 생성된 파라미터를 기반으로 세션키를 생성 후 안전한 통신을 수행하도록 하며, 권한 관리 프로토콜을 설계하여 신뢰성 있는 통신 프로토콜을 설계하도록 한다.

본 논문은 5장으로 구성되어 있다. 2장에서는 클라우드 기반의 빅 데이터 융합기술 활용사례와 보안위협 요구사항에 대해서 관련연구를 수행한다. 3장에서는 접근제어 및 권한관리 프로토콜을 설계하고 4장에서는 이에 대해 안전성 분석, 보안성 및 효율성을 평가한다. 5장에서는 결론과 향후 연구방향성을 제시한다.

2. 관련연구

2.1 클라우드 기반의 빅데이터 융합기술 활용 사례

전 세계적으로 클라우드 시장의 규모는 지속적으로 확대되고 있으며, 국내 기관•기업에서도 가파른 상승세를 기록 중이다. 2015년 3월을 계기로 민간 클라우드 서비스를 도입함으로써 사용자들로부터 다양한 분야의 서비스를 제공하고 있다. IT 시장 내의 빅 데이터, IoT와 같은 신기술이 융합되는 서비스가 나타나면서 기반기술인 클라우드 산업에 대한 연구가 활발히 진행되고 있다[4,7,13,15].

융합 IT기술이 주도함으로써 다양한 서비스와 기술력들이 생성되어 산업부분에서 새로운 패러다임이 제시되고 있다. 기존의 단독적인 IT 기술이 아닌 의료, 농업, 건축, 수산업등과 같은 다른 분야와 맞물려서 신기술 서비스가 생겨나고 있다.

대형 스토리지 기반의 클라우드 컴퓨팅 서비스 시스템은 하이브리드 방식으로 서비스를 수행을 살펴보면 캐쉬 메모리(DRAM) + HDD, 캐쉬 메모리(DRAM+Flash) + HDD, DRAM-SSD + HDD 스토리지 시스템을 사용하여 입/출력 속도를 높이고 있다[5].

클라우드 컴퓨팅 환경과 빅 데이터 기반의 기술이 융합된 사례를 살펴보면 3만 명 이상의 학생, 교직원이 교육 및 연구 수행과정에서 컴퓨터 스토리지에 대한 배분을 효과적으로 사용하여 75%의 라이선스 비용을 절감하고 있다. 또한 의료 환경에서는 통계 자료를 기반으로 정확한 환자수 및 진료비를 추정 및 분석하여 의사, 의료업체로 하여금 효율성 있는 서비스를 제공하도록 기여하고 있다[6,7].

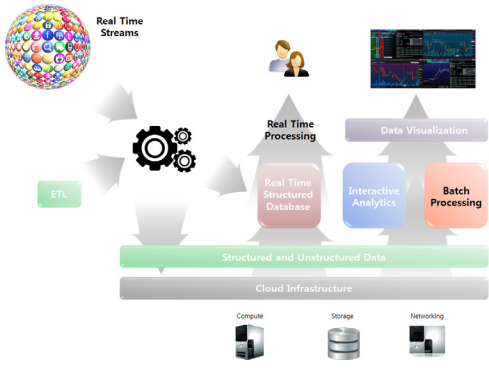

Fig. 1. Configuration of Convergence Server based Big data in Cloud Computing Environment

2.2 클라우드 및 빅데이터 보안위협 및 요구사항

클라우드 컴퓨팅 기술은 사용자가 별도의 소프트웨어

없이 유•무선 네트워크 환경에서 원하는 서비스를 이용할 수 있으며, 별도의 저장장치가 필요 없이 손쉽게 사용할 수 있다는 장점이 있다. 하지만 스토리지 서비스의 보안위협이 발생하면 사용자의 개인정보가 유출되고, 가용성에 위협된 공격을 받으면 서비스를 지원받을 수 없다는 단점이 있다. 국외기업 A사에서는 11시간 동안 서비스가 중단되어 금융적인 부분에서 막대한 피해가 발생한 적이 있어, 사용자가 데이터를 저장하는 부분에서 불신감을 가지고 있다[7,12].

클라우드 환경에서 발생하는 위협오소를 살펴보면 클라우드 컴퓨팅 서비스의 남용과 불손한 사용, 안전하지 않은 인터페이스와 API, 악의적인 내부자들, 기술 문제의 공유, 데이터 손실, 하이재킹 등이 있다. 클라우드 기반 기술에서는 하드웨어, 스토리지, 네트워크 가상화 기반의 핵심기술이 존재하는데, 악의적인 사용자 및 공격자들로부터 타깃이 될 수 있다. 이를 보안하기 위해서 보안 정책의 구현, 클라우드 환경의 모니터링, 인증 및 액세스 제어, 취약성 검사 및 감사 등에 대한 연구가 필요하다[8,14].

클라우드 컴퓨팅 환경에서 “Assessing the Security Risks of Cloud Computing”따르면 접근권한에 관한 정보, 규정준수, 데이터의 위치, 데이터 분리여부 파악, 데이터 복구, 불법행위 등에 대한 조사, 기업의 지속성에 대해서 발표를 하였다. 미 정부 가이드라인 “FedRAMP Security Controls Baseline v1.0”(FedRAMP)에서는 클라우드 컴퓨팅 보안요구 기준, 지속적인 모니터링, 평가 및 인가 프로세스에서 명시하였다[8].

3. 제안 프로토콜

본 장에서는 클라우드 컴퓨팅 환경에서 콘텐츠 접근제어 및 권한 관리 프로토콜을 제안하였다. 제안 시스템은 사용자, Agent, Authority Server, Storage Server로 구성되어 있다. 사용자는 클라우드 컴퓨팅환경의 Storage의 콘텐츠를 접근하기 이전 등록 및 권한을 부여받는다. 이후 이전에 등록된 파라미터를 기반으로 통신을 수행한다. 통신 수행과정에서 권한 등급 및 사용자 정보가 만료되었을 때 갱신 프로토콜을 수행하는 방식이다. 제안된 프로토콜의 약어 표는 [Table 1]과 같다.

Table 1. Abbreviation

Abbreviation	Description
$User_{i-ID}$	ID of User
$User_{i-PWD}$	Password of User
$User_{parameter}$	Parameter of User
$Cert_{Value}$	Certification of Agent
$User_{i-nonce}$	Generate of Device` nonce
$User_{grade}$	Grade of User
$Grade_{factor}$	Authority Server generate grade factor
$User_{value}$	Valid Value of User
$Session_{key}$	Session Key

3.1 사용자 등록 및 권한 부여 프로토콜

클라우드 환경에서 빅데이터 기반의 통신을 수행하기 이전 사용자 등록 및 등급에 알맞은 권한을 부여하는 단계이다. 사용자의 정보를 확인하고 유효값을 검증 후 $Grade_{factor}$를 생성한다. 이후 Agent에서는 검증완료메시지를 수신 후 등록함으로써 본 절의 프로토콜을 도시화 하며 상세 프로토콜은 [Fig. 2]와 같다.

1. 사용자는 Agent로부터 등록 요청 메시지를 전송한다.
   $User_{i-ID}, Pub_{AS}(User_{i-PWD})$
2. Agent에서는 사용자의 ID를 검사 후 Authority Server로 검증요청 메시지를 전송한다.
   $User_{i-ID}, Pub_{AS}(User_{i-PWD}), Pub_{AS}(Cert_{Value})$
3. Authority Server는 수신된 메시지를 복호화 후 사용자 ID와 Agent의 인증 값을 검증한다.
4. Authority Server에서는 Agent를 경유하여 User로부터 유효값을 요청한다.
5. 사용자는 파라미터를 추출하고 난수를 생성 후 유효값을 계산한다.
   $User_{Value} = Hash(User_{i-nonce} \oplus User_{Parameter} \| PAD)$
6. 사용자는 공개키로 암호화 후 Agent를 거쳐서 Authority Server로 유효값 응답 메시지를 발송한다.
   $Pub_{AS}(User_{Value}, User_{i-nonce})$
7. Authority Server는 수신된 메시지를 검증 후 사용자의 유효값을 계산한다. 이후 사용자의 등급 값을 생성 후 저장하고 $Grade_{factor}$를 생성한다.
   $Grade_{Factor} = (User_{grade}) \oplus Cert_{Value}$
8. Authority는 Agent로 검증 완료 메시지를 전송한다.
   $Pub_{A}(Grade_{factor}, User_{i-nonce}, Time\,Stamp)$

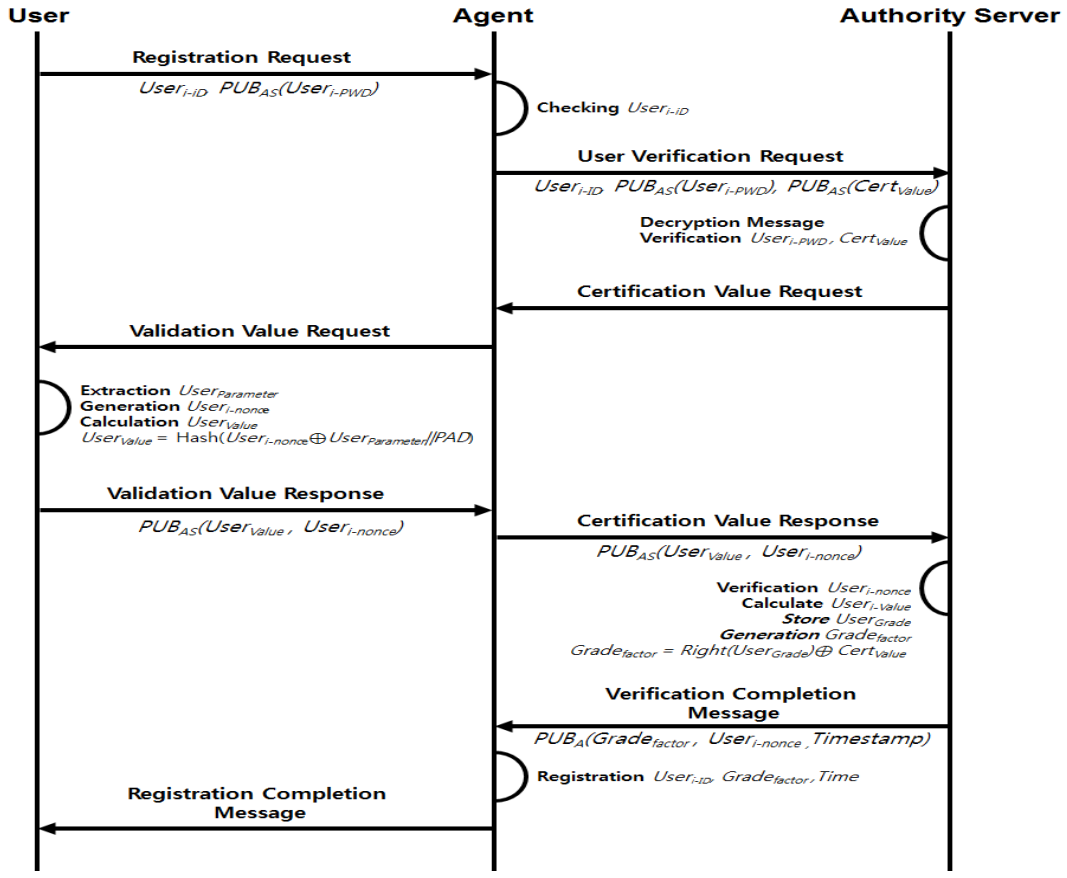

Fig. 2. User Registration and Authority Grant

9. Agent는 수신된 메시지를 복호화 후 ID, $Grade_{factor}$, Time을 등록한다.

3.2 메시지 통신 프로토콜 설계

이전의 등록 및 권한 부여 프로토콜에서 생성된 파라미터를 기반으로 안전한 통신을 수행한다. 사용자는 Storage Server로 접근 후 데이터를 검색한다. Agent에서는 이전의 생성된 서명값, 난수값과 같은 파라미터 기반으로 $Session_{Key}$를 생성하여 통신절차를 수행한다. 상세프로토콜은 [Fig. 3]과 같다.

1. 사용자는 Agent로 로그인 요청을 수행 후 클라우드 컴퓨팅 Storage Server의 데이터 항목을 읽는다.

$User_{i-ID}, PRI_{User}(User_{Value})$

2. Storage Server에서는 데이터 항목을 Agent로 전송 후, Authority Server로부터 권한 요청 메시지를 전송 한다.

3. 권한 요청 메시지를 받은 Authority Server는 서명값을 복호화 후 시간, 사용자 ID, 유효값을 검증한다. 이후 클라우드 컴퓨팅 Storage Server완료 메시지를 전송한다.

4. 검증이 완료되면 Agent로 데이터를 전송 하고, Agent에서는 세션키를 생성 한다.

$Session_{key} = Hash(Hash(\mathrm{Pri}_{user}(User_{value})) \oplus User_{i-nonce})$

5. 생성된 세션키로 암호화 후 데이터를 발송한다. 통신과정이 끝나면 세션키를 폐기한다.

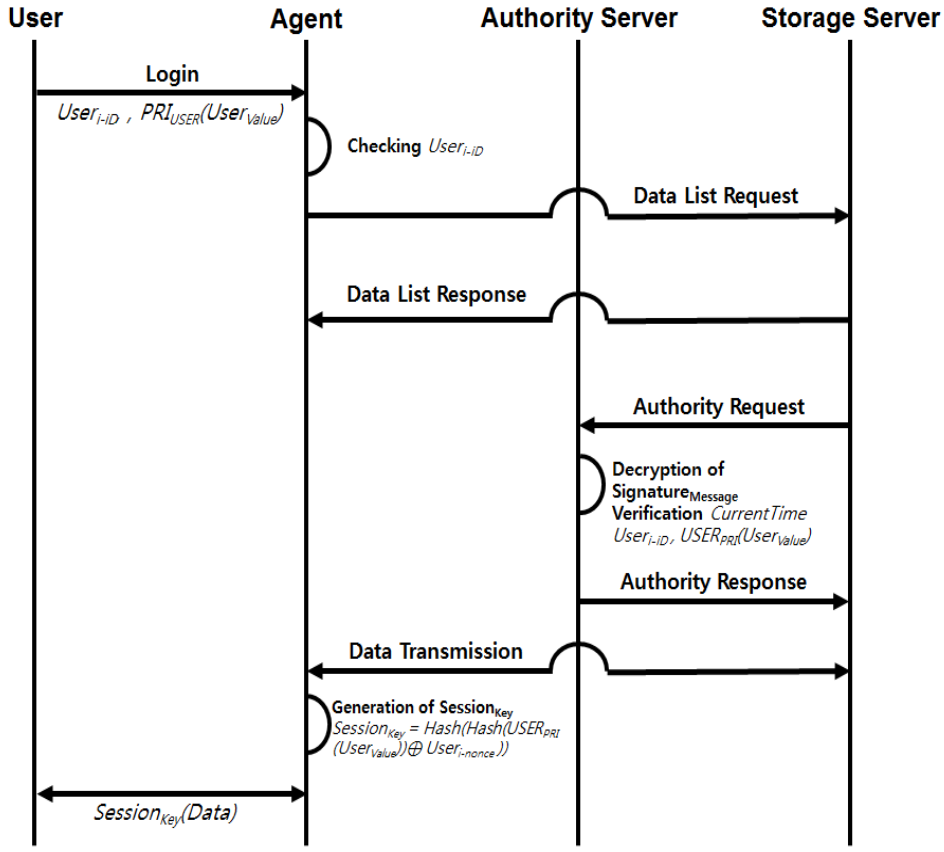

Fig. 3. Message Communication Protocol

3.3 갱신 및 권한 관리 프로토콜 설계

본 절에서는 사용자의 권한 관리를 수행한다. 사용자 권한에 따른 등급을 갱신하여 Storage Server의 접근제어에 대한 보안성을 강화하는 프로토콜을 설계한다. 등록 프로토콜에서 생성된 파라미터를 비교 • 분석을 수행하여 $Grade_{Factor}$에 대한 보완하여 안전성을 확보한다. 상세 프로토콜은 [Fig. 4]와 같다. Agent는 사용자로부터 유효값을 요청 후 사용자는 유효값을 응답한다.

$User_{i-ID}, User_{\mathrm{Pr}i}(User_{Value})$

1. Agent는 사용자 아이디와, 시간을 검사한다. 이후 Authority Server로 사용자 아이디, 인증 값을 개인키로 암호화 후 서명 값을 전송한다.
$User_{ID}, PRI_A(Cert_{value})$

2. Authority Server는 Agent를 경유하여 사용자로부터 갱신값을 요청한다.

3. 사용자는 난수를 생성하고 유효값을 생성 후 Agent를 거쳐서 Authority Server로 발송한다.
$User_{Value} = Hash(User_{i-nonce} \oplus User_{parameter} \| PAD)$

4. Authority Server에서는 $Grade_{Factor}$, $User_{i-nonce}$를 검증하고 유효값을 계산한다. 이후 사용자 등급을 저장하고 $Grade_{Factor}$를 생성한다.
$Grade_{factor} = (Exist(Grade_{Factor}) \oplus User_{grade}) \oplus Cert_{value}$

5. Authority Server는 Agent로 갱신 완료 메시지를 전송한다. 이후 Agent에서는 사용자 아이디, $Grade_{Factor}$와 시간을 등록한다.
$Pub_A(Grade_{factor}, User_{i-nonce}, Timestamp)$

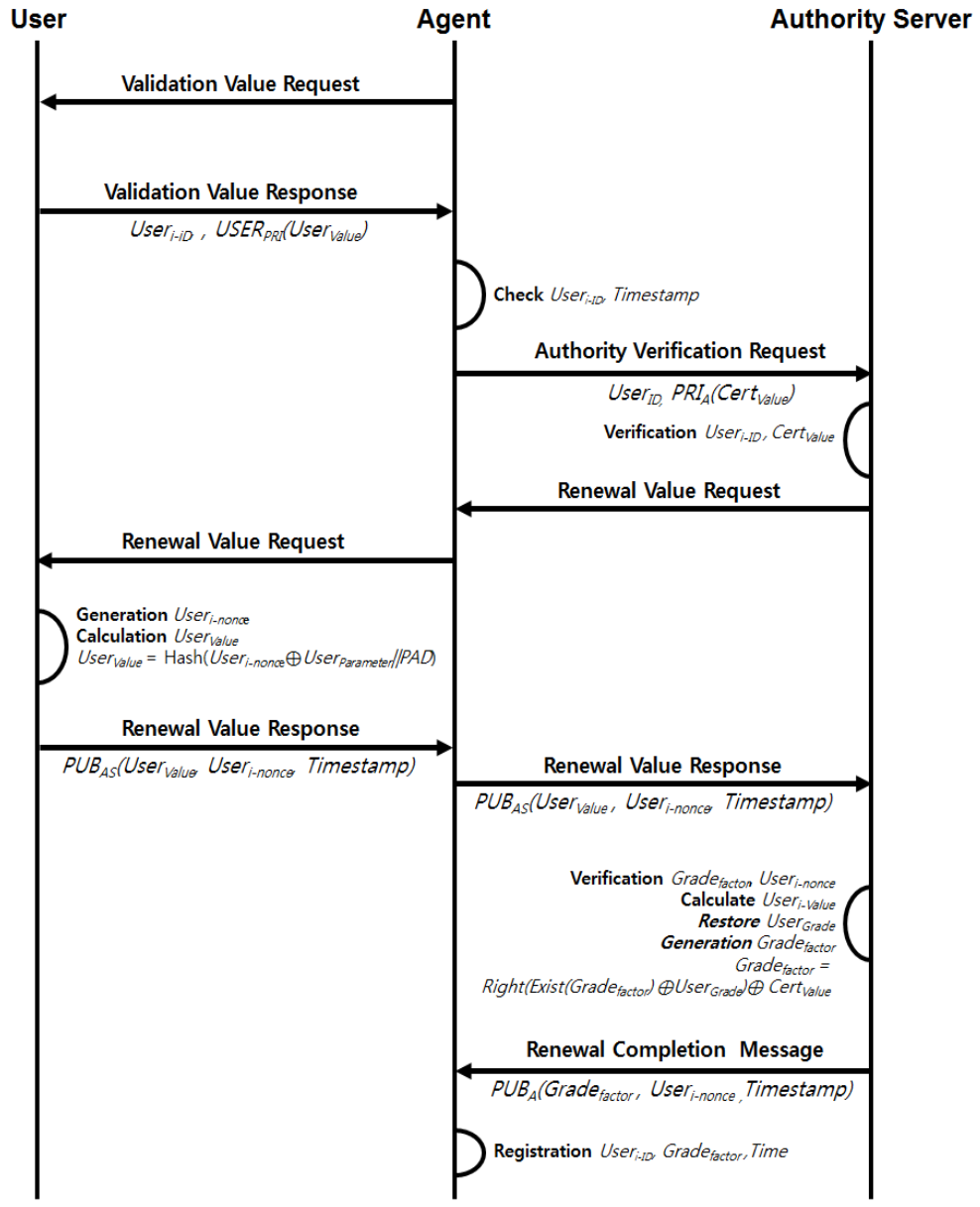

Fig. 4. Renewal and Authority Management Protocol

4. 제안 프로토콜

4.1 안전성 분석

4.1.1 비 인가된 사용자 접근

빅 데이터 기반의 데이터 스토리지 기술에서는 비인가 된 사용자의 접근제어 기술이 요구되며, 디바이스에 대한 검증 및 인증 절차가 필요하다. 이를 보완하기 위해서 디바이스 등록단계에서 $User_{Value}$ 을 검증하고, 메시지 통신단계에서 $PRI_{User}(User_{Value})$의 서명 값을 검증함으로써 비 인가된 사용자의 접근이 불가능하다.

4.1.2 데이터 기밀성 위협 및 무결성 침해

클라우드 환경의 빅 데이터 통신과정에서 데이터에 대한 무결성이 보증되어야 하고 안전하게 통신되어야 한다. 메시지 통신단계에서 $User_{value}$, $User_{i-nonce}$을 기반

으로 세션 키를 생성 후 암호화하여 전송함으로써 안전하게 통신이 수행할 수 있다. 또한 데이터의 유효값 및 $Grade_{factor}$를 검증함으로서 데이터의 무결성에 대한 침해를 방지할 수 있다.

4.1.3 중간자 공격 및 위장 공격

공격자가 Agent를 위장하여 송신되는 데이터를 탈취하는 위장 • 중간자 공격은 클라우드 환경뿐만 아니라 네트워크 환경에서 발생하는 공격기법이다. 이를 방지하기 위해서 Authority Server에서 사용자의 인증값, 유효 값과 생성한 난수 값을 개인키로 암호화하여 $Signature_{message}$을 검증함으로써 위장공격에 대한 위협을 보완하였다. 그리고 $Session_{Key}$를 생성과 갱신 프로토콜을 설계하여 중간자 공격을 막을 수 있다.

4.1.4 내부자 정보유출 방지

클라우드 환경 및 BYOD 기술을 도입하고 있는 기관, 기업에서는 정보유출에 대한 피해사례가 발생하고 있다. 이를 방지하기 위해서 본 논문에서는 사용자 등록 관리에서 Authority Server에서 $Grade_{factor}$ 값을 생성하여 권한등급에 따른 접근체계를 설계하였다. 그리고 갱신 및 권한 관리 프로토콜을 설계하여, 갱신된 $User_{i-nonce}$를 통신하여 $Grade_{factor}$을 등급 수정, 갱신과 시간을 등록하여 통신을 수행함으로써 내부자의 정보유출을 방지하였다.

4.2 보안성 및 효율성 평가

Java언어 환경에서 JCE기반의 기존의 암호 시스템(AES, SEED)과 제안된 암호시스템의 성능 평가를 수행하였다. 기존의 시스템에서는 인증과정 및 해쉬과정과 세션키(대칭키 암호)와의 수행속도를 비교한 결과를 [Fig. 5], [Fig. 6]에서 나타내었다.

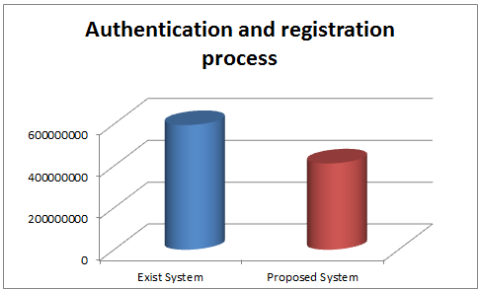

Fig. 5. Cipher Performing Analysis

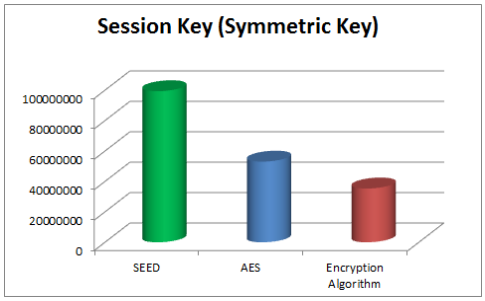

Fig. 6. Symmetric Key Analysis

기존의 암호시스템 대비 제안된 시스템에서는 대략 55%의 향상률을 보였으며, 세션키에서는 SEED, AES와 대략 35%, 66%대비 수행속도저하를 확인할 수 있었다. 기존의 시스템과 보안성에 관하여 클라우드 환경에서 스토리지 접근제어 기술의 FedRAMP기반으로 보안요구를 분석하였다. 기밀성, 무결성, 상호인증, 권한관리, 접근제어, 유지관리에서 보안성을 분석하였고 결과는 [Table 2]와 같다.

Table 2. Comparison of Exist Cloud Computing Environment And Proposed System

Separate	Exist Cloud Computing System	Proposed System
Confidentiality	Support	Support
integrity	Support	Support
Identification and Mutual Authentication	Support	Support
Rights Management		Support
Access Control		Support
Maintenance Management		Support

제안된 시스템과 기존의 클라우드 환경에서 신분증명 및 인증, 권한관리, 접근제어, 유리 관리부분에서 강화하였다. 미 정부 가이드라인 “FedRAMP Security Controls Baseline”의 보안 요구기준과 지속적인 모니터링을 강화하도록 설계하였다.

5. 결론

본 논문에서는 클라우드 환경의 콘텐츠 접근제어 및

권한 관리 프로토콜에 관하여 연구하였다. 제안 프로토콜에서 사용자 등록 및 권한 등급 부여 프로토콜을 설계하여 이를 기반으로 안전한 통신을 수행하도록 연구하였다. 또한 통신 프로토콜에서 안전한 메시지를 사용자로부터 전송하고 내부 유출 강화하기 위해서 세션키를 생성하였다. 클라우드 서버 Storage Server의 콘텐츠의 안전성을 강화하기 위해서 파라미터 갱신 및 권한 관리 프로토콜을 설계하여 접근제어를 강화하였다.

클라우드 환경에서 발생하는 보안위협 및 공격기법을 기반으로 안전성을 분석하였으며, FedRAMP기반으로 보안성을 평가하였다. 기존의 암호방식과 세션 키(대칭키) 부분의 효율성을 분석하여 55%의 향상된 값을 확인할 수 있었다.

빅데이터 기반 융합기술 환경에서 제안된 시스템을 도입하기 위해서 권한관리, 인증 및 유지관리 기술뿐만 아니라 사고대응, 위협 측정에 대한 기술이 요구되며 보안경고 및 교육에 따른 보안 정책이 필요하다. 향후 제안된 시스템을 강화하여 콘텐츠 내부 보호와 평가와 권한인가를 보완할 수 있는 기술 및 정책이 요구된다.

References

[1] T. H Shin, K. G. Seo, “The Convergence Services Cases on Cloud Computing”, Cloud Computing Support Center, 2014.

[2] S. A. Shin, K. E. Kim, “Big Data technology classification and status”, NIA, KBig Center, 2013.

[3] H, J, LEE, D. H Won, “An Analysis of Cloud System Security Functional Requirement”, vol. 6, no. 9, 2012.

[4] FedRAMP, “FedRAMP Security Control Baseline v1.0” 2012.

[5] FedRAMP,“FedRAMP CONOPS”, February. 2012.

[6] So-Yeon Min, Byung-Wook. Kwang-Hyoung Lee, “A Study for Key Generation and Access Control Protocol in BYOD Environments”, KOCON, vol. 15, no. 5, pp. 27-36, 2015.

[7] S. H. Koo, M. S. Shin, “A Study on the Enhancement Process of the Telecommunication Network Management using Big Data Analysis”, KAIS, vol. 13, no. 12, pp. 6060-6070, 2012.
DOI: http://dx.doi.org/10.5762/kais.2012.13.12.6060

[8] Jong-Hun Park, Gang-Seong Lee, Sang-Hun Lee, “A Study on the Convergence Technique enhanced GrabCut Algorithm Using Color Histogram and modified Sharpening filter”, Journal of the Korea Convergence Society, vol. 6, no. 6, pp. 1-8, 2015.
DOI: http://dx.doi.org/10.21562/kjs.2015.04.49.2.1

[9] Byeong Ho Knag, Tai-hoon Kim, “Effective Optimization of Multi-Clouds using Software-as-a-Service,” Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 2, no. 2, pp. 85-92, Dec. 2012.
DOI: http://dx.doi.org/10.14257/AJMAHS.2012.12.04

[10] Yvette E. Gelogo, H.-K. Kim, “Enterprise Resource Planning System Deployment on Mobile Cloud Computing,” Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 3, no. 1, pp.1-8, June 2013.
DOI: http://dx.doi.org/10.14257/AJMAHS.2013.06.02

[11] C.-H. Park, J.-K. Kim, J.-G. Yoo, N.-Y. Lee, J.-B. Kim, “A Study on the Cloud Computing Service for Education Organization,” Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 6, no. 1, pp. 29-38, Jan. 2016.
DOI: http://dx.doi.org/10.14257/AJMAHS.2016.01.32

[12] J. Y. Hwang, S. K, Jeong, “Big Data, Cloud Computing, and High-end Hybrid Storage Systems Technology Trend and Market“, KIOS, Spring Conference, 2012.

[13] Hyun-Sook Chung, Jeong-Min Kim, “Design of Semantic Models for Teaching and Learning based on Convergence of Ontology Technology”, Journal of the Korea Convergence Society, vol. 6, no. 3, pp. 127-134, 2015.
DOI: http://dx.doi.org/10.15207/JKCS.2015.6.3.127

[14] Bo-Kyung Lee, “A Study on Security of Virtualization in Cloud Computing Environment for Convergence Services”, Journal of the Korea Convergence Society, vol. 5, no. 4, pp. 93-99, 2014.
DOI: http://dx.doi.org/10.15207/JKCS.2014.5.4.093

[15] Julie Kim, Hyokyung Bahn, “An Efficient Log Data Management Architecture for Big Data Processing in Cloud Computing Environments,” The Journal of The Institute of Internet, Broadcasting and Communication vol. 13 no. 2, pp. 1-7, 2013.
DOI: http://dx.doi.org/10.7236/JIIBC.2013.13.2.1

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 정보통신, 클라우드 서비스

이 광 형(Kwang-Hyong Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 (공학사)
- 2002년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 인터넷 정보과 부교수

<관심분야>
멀티미디어 보안, 사물인터넷, 학습콘텐츠, 영상처리

진 병 욱(Byung-Wook Jin) **[정회원]**

- 2010년 2월 : 청운대학교 멀티미디어학과 (문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2013년 3월 : 숭실대학교 컴퓨터학과 박사수료

<관심분야>
사물지능통신, 인증, 접근제어