빅데이터 환경에서 정부민원서비스센터 어플리케이션 불법 이용에 대한 서비스 자료 암호화 모델

김명희* · 백현철** · 홍석원*** · 박재홍****

요 약

최근 정부 민원 행정 시스템은 단순한 네트워크 환경에 의한 민원 서비스에서 클라우드 컴퓨팅 환경으로 진화하고 있다. 오늘 날 방대한 양의 전자 민원 서비스 처리 환경은 클라우드 컴퓨팅 환경을 기반으로 하는 빅데이터 서비스를 의미한다. 그러므로 이러한 정부 민원 행정 서비스 업무를 위한 빅 데이터 처리 과정은 기존 정보 수집 환경에 비해 많은 문제점을 가지고 있다. 즉, 기존 네트워크 환경에서의 정보 서비스 차원을 넘어 다양한 정보 시스템으로부터 필요 정보를 수집하고 이를 통한 새로운 정보를 가공해 내는 과정을 거친다. 이에 따라 방대한 양의 빅 데이터 서비스 처리를 위한 행정 정보 제공 어플리케이션들은 불법적인 공격자들의 집중적인 표적이 되고 있는 실정이다. 본 논문은 전국 각지의 민원서비스 센터의 IP를 이용하여 전자민원 서비스 업무를 수행하는 어플리케이션의 불법적인 이용과 이들이 보유하고 있는 중요 정보 유출을 막기 위한 모델이다. 본 논문에서는 이를 위하여 다양한 인증과정과 이를 통한 암호화 방법을 제시하여 서비스의 안정성과 가용성, 기밀성을 유지할 수 있도록 하였다.

An Encrypted Service Data Model for Using Illegal Applications of the Government Civil Affairs Service under Big Data Environments

Kim Myeong Hee* · Baek Hyun Chul** · Hong Suk Won*** · Park Jae Heung***

ABSTRACT

Recently the government civil affairs administration system has been advanced to a cloud computing environment from a simple network environment. The electronic civil affairs processing environment in recent years means cloud computing environment based bid data services. Therefore, there exist lots of problems in processing big data for the government civil affairs service compared to the conventional information acquisition environment. That is, it processes new information through collecting required information from different information systems much further than the information service in conventional network environments. According to such an environment, applications of providing administration information for processing the big data have been becoming a major target of illegal attackers. The objectives of this study are to prevent illegal uses of the electronic civil affairs service based on IPs nationally located in civil affairs centers and to protect leaks of the important data retained in these centers. For achieving it, the safety, usability, and security of services are to be ensured by using different authentication processes and encryption methods based on these processes.

Key words : Big data, Big data security, Cloud Computing, Computer network, Encryption, Traceback

접수일(2015년 11월 16일), 게재확정일(2015년 12월 18일)

* 경상대학교 컴퓨터과학과(책임저자)
** 경남도립남해대학 스마트융합정보과
*** 경남도립거창대학 교무부
**** 경상대학교 컴퓨터과학과(교신저자)

1. 서 론

최근 정부 민원 행정 시스템은 초기 단순 송/수신 자간의 네트워크 환경을 통한 민원 서비스에서 클라우드 컴퓨팅 환경으로 진화하고 있다.[8][9] 오늘 날 방대한 양의 전자 민원 서비스 처리 환경은 이러한 클라우드 컴퓨팅 환경을 기반으로 하는 빅데이터 서비스를 의미한다고 할 수 있다. 클라우드 컴퓨팅 기술에 기반한 정부 민원 행정 서비스 업무를 위한 빅데이터 처리 과정은 기존 정보 수집 환경에 비해 많은 문제점을 가지고 있다. 즉, 기존 네트워크 환경에서의 정보 서비스 차원을 넘어 다양한 정보 시스템으로부터 필요 정보 수집을 한다. 그리고 이를 통하여 새로운 정보들을 가공해 내는 과정을 거치기 때문에 포괄적인 정보 수집과 처리과정이 반드시 필요하다.

아울러 방대한 양의 빅 데이터 서비스 처리를 위한 행정 정보 제공 어플리케이션들은 불법적인 공격자들의 집중적인 표적이 되고 있는 실정이다.

본 논문에서는 전국 각지의 민원서비스 센터의 IP를 이용하여 전자민원 서비스를 위한 어플리케이션의 불법적인 이용과 이들이 보유하고 있는 중요 정보 유출을 막기 위하여 다음과 같은 인증과정을 이용한 암호화 방법을 제시하였다. 먼저 IP Spoofing를 이용한 공격자들의 불법적인 접근에 대비하여 트레이스 백 정보를 이용하여 초기 접근과 관련한 인증 정보로 사용하였다. 그 다음 정상 사용자의 직원 코드, 해당 사용자의 어플리케이션 이용 권한 코드를 이용하여 해당 어플리케이션에 대한 접속과 실행여부를 판정하고, 적절한 암호화를 실시하도록 하였다.

이를 위하여 전자민원 서비스를 실시하는 각 어플리케이션에 코드 값을 부여하고, 해당 어플리케이션 접속에 대한 이용자 검증을 통하여 불법적인 전자 민원서류 요청에 대응할 수 있도록 하였다. 이는 특정인의 부당한 개인 정보 유출로 인하여 발생할 수 있는 소중한 개인 정보 및 재산상의 문제를 범죄로 부터 보호할 수 있도록 하기 위함이다.

본 논문의 구성은 다음과 같다. 2장에서 빅 데이터와 관련된 연구를 살펴보고, 3장에서는 빅 데이터 환경에서의 보안 모델을 제안하고 그 동작 과정을 설명하였다. 4장에서는 이에 대한 시뮬레이션과 제안 모델의 보안 레벨에 대한 단계별 보안 정책을 수행하였다. 그리고 결론에서 향후 본 논문의 응용 가능성에 대한 언급을 하였다.

2. 관련연구

2.1 빅 데이터의 개념 정의

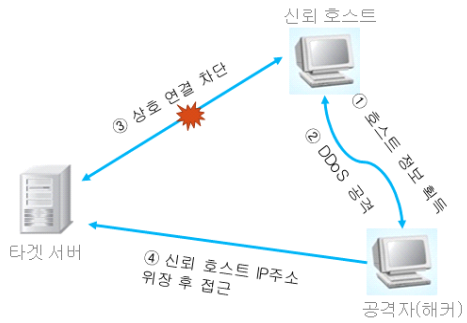
빅 데이터에 대한 정의는 최근 빅 데이터에 대한 다양한 연구 사례를 통하여 그 정의를 분석해 볼 수 있다. 그 중 가장 일반적인 분석은 기존 분석도구나 시스템 체계에서 처리 가능한 범위를 넘어선 방대한 양의 데이터 환경을 빅 데이터로 정의하고 있다. 아울러 또 다른 시각의 빅 데이터 개념으로는 다양한 종류의 대규모 데이터로부터 저렴한 비용으로 가치 추출이 가능하고, 필요 데이터에 대한 빠른 수집과 발굴 및 분석을 할 수 있는 차세대 기술 또는 아키텍처를 의미하기도 한다.[1]

이상과 같이 빅 데이터 환경에 대한 개념 정의를 통하여 알 수 있듯이, 중요 자료 유출에 대한 보안의 문제는 오늘 날 더욱 요구된다고 할 수 있다. 특히 클라우드 컴퓨팅 기반의 정보 수집 과정의 특성상, 고도의 해킹 기술을 이용하는 공격자들이 이용 가능한 IP Spoofing 공격에 대한 대응 기법이 필요한 시점이라고 할 수 있다.

2.2 IP Spoofing 공격

IP Spoofing이란 자신의 IP를 속여 불법적인 접근을 시도하는 것을 뜻한다. IP 스푸핑은 TCP/IP의 구조적인 결함에서 출발한 방법으로 TCP의 시퀀스 번호, 소스 라우팅 정보, 소스 IP 주소를 이용하여 (그림 1)과 같이 상대방 호스트가 공격자 자신의 호스트를 신뢰하게 만드는 방법이다. IP Spoofing 공격을 단계별로 살펴보면 먼저 공격자가 타겟 서버에 접속하기 위해 타겟 서버와 신뢰 관계를 가지고 있는 임의의 신뢰 호스트의 정보를 획득한 후 해당 호스트에 DoS나 DDos 공격을 이용하여 해당 호스트를 다운시킨다. 그 다음 타겟 서버와 해당 신뢰 호스간의 네트워크 연결이 해제되면, 공격자가 해당 신뢰 호스트의 IP 주

소를 자신이 재설정하고 타겟 서버로 접근하여 정보를 빼내가는 것이다. 이렇듯 상호 IP 주소를 통한 신뢰 관계를 이용하여 공격을 시도하기 때문에 방어 기법이 아주 어렵다고 할 수 있다. [2][3]



(그림 1) IP Spoofing 공격의 예

2.3 클라우드 컴퓨팅의 개념

클라우드 컴퓨팅에 대한 정의는 각 기관이나 학자마다 그 견해가 다르다. 그렇지만 공통된 점을 분석하여 정의해 보면 '네트워크 환경에서 이용자의 요구에 따라 실시간으로 소프트웨어, 플랫폼, 인프라 등 IT 자원이 필요한 만큼 공급받고, 그에 따른 비용을 지불하는 서비스'라고 정의할 수 있다. 이러한 클라우드 컴퓨팅 환경은 개인이나 기업, 공공기관 등의 보안 시스템 환경의 변화도 요구하고 있다. 아울러 공격자들의 공격기법도 빠르게 변하고 있다. 그러므로 행정 민원서비스를 위한 클라우드 컴퓨팅 환경 하에서 발생 가능한 다양하고 불법적인 공격으로부터 중요한 정보자산을 보호하기 위한 대응 기법이 새롭게 요구되고 있는 실정이다[4].

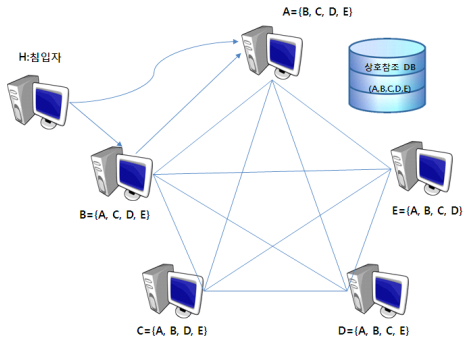
2.4 트레이스 백 정보의 개념

일반적인 네트워크 과정은 출발지에서 목적지까지 여러 개의 경로를 거쳐 연결되는 과정을 가지고 있다. 트레이스 백 정보란 이러한 네트워크 경로 분석을 위하여 사용하는 프로그램이다. 즉, 특정 컴퓨터가 네트워크 과정을 통하여 최종 목적지까지 도달할 때 까지 경유하는 각 구간 정보를 기록하는 프로그램이다. 본 논문에서는 트레이스 백 정보를 이용하여 각 구간 경로 정보를 분석한 후 원격 접속을 시도하는 사용자들에 대하여 인증 과정 정보로 이용하고 있다.[5]

3. 제안 모델 설계

3.1 제안 모델

본 논문에서 제안하는 IP Spoofing 공격에 대한 정보 제공 시스템들의 상호 협력 모델은 다음과 같은 구조를 가지며 (그림 2)로 나타내었다.



(그림 2) 상호협력시스템

(그림 2)에서 A, B, C, D, E는 클라우드 컴퓨팅 환경에서의 상호 정보 제공을 실시하는 각 민원 서비스 센터들의 시스템을 의미하고 H는 IP Spoofing 공격을 이용한 불법접근자로 가정하였다. 아울러 정보 제공 시스템들은 자신을 제외한 다른 협력 시스템으로부터 정상적인 접속을 시도하는 시스템들의 상호 트레이스 백 정보와 해당 사용자들의 직원코드, 민원 서비스를 위한 어플리케이션들의 등급 정보를 가진다. 본 논문에서 각 민원 서비스 센터는 다양한 민원 서비스 업무를 실시하고 있기 때문에 <표 1>과 같은 코드 값을 부여하여 관리할 수 있도록 하였다. 즉, 민원 서비스 센터는 부서별로 업무가 분리되어 있기 때문에 서비스 담당자들의 고유 ID와 접근 가능한 어플리케이션 정보를 사용자별로 등록하여 불법적인 접근에 대응하기 위함이다.

<표 1> 직원코드별 이용 어플리케이션 목록

직원 코드	민원 서비스를 위한 어플리케이션 코드	어플리케이션 등급
A_01	A01_prg_1	1
	A01_prg_2	2
	A01_prg_3	3
B_01	B01_prg_4	1
	B01_prg_5	2
	B01_prg_6	3
C_01	C01_prg_7	1
	C01_prg_8	2
	C01_prg_9	3
·	·	·
·	·	·
N_n	N01_prg_n	1 ~ 3

본 논문에서는 <표 1>의 정보를 이용하여 IP Spoofing 공격이 발생하게 되면 적절한 인증 과정을 거치도록 하였다. 아울러 2등급 어플리케이션 중 향후 2등급 어플리케이션을 이용한 자료 조합이 발생할 경우에 대비하여 암호화 과정을 수행할 수 있도록 하였다.

빅 데이터 서비스를 위한 민원 서비스 센터의 운영은 일반적으로 여러 시스템이 보유하고 있는 자료들을 이용하여 다양한 서비스를 제공한다. 공격자는 어플리케이션 사용 권한을 가지고 있는 직원들의 코드를 이용하여 유용한 정보를 불법적으로 유출하려고 한다. 본 논문에서는 2개 이상의 직원코드를 이용하여 어플리케이션을 통한 불법적인 자료 유출을 시도할 때 유출 자료가 동일인에 대한 내용 인지 여부를 검증하여 이에 대응할 수 있도록 하였다.

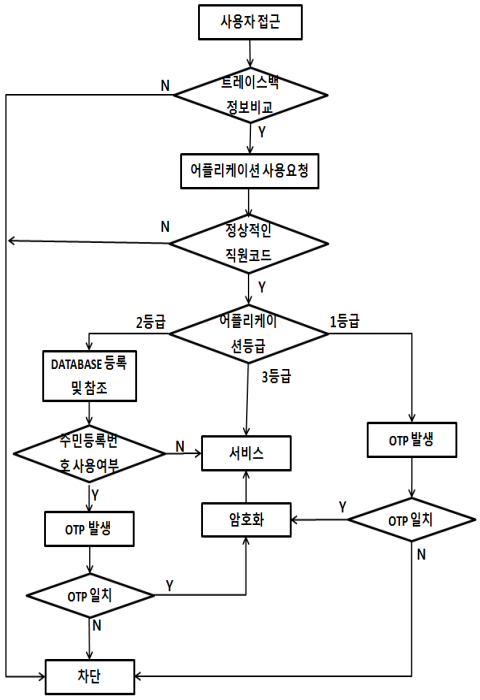
본 논문의 (그림 2)에서 서비스 실시를 하고 있는 시스템 A, B, ... , Z에서 관리하는 어플리케이션들은 상호 다른 2등급 어플리케이션 자료와의 조합이 발생할 가능성이 있다. 이 경우 2개 이상의 2등급 어플리케이션으로부터 추출한 자료가 1등급 어플리케이션 추출 자료로 전환할 수 있다. 본 논문에서는 하나의 2등급 어플리케이션에 대한 접근이 발생하면 이들 접근 정보를 상호 참조 가능한 사용자 어플리케이션 접근 데이터베이스에 생성해 두었다. 그리고 이를 위하여 서비스 어플리케이션의 접근 자료 항목의 주민번호를 이용하여 동일인 여부를 비교 검증하고 두 번째 어플리케이션 서비스 자료부터는 암호화를 시행하도록 하였다. 아울러 1등급 어플리케이션 서비스 자료는 중요도가 높은 자료이기 때문에 해당 자료를 반드시 암호화 시킨 후 서비스 요청자에게 전송한다. 3등급 어플리케이션 서비스 자료는 일반적인 서비스 자료이므로 별도의 암호화 작업 없이 서비스를 실시하도록 한다.[6][7]

3.2 제안 모델 동작과정

본 논문에서 제안하고 있는 모델의 사용자 접근 처리 과정은 (그림 3)과 같다. 클라우드 컴퓨팅 기반의 빅데이터 서비스 환경은 그 특성상 IP Spoofing 공격이 발생할 가능성이 높다. 그러므로 사용자 접근이 발생하면 각 민원 서비스는 자신이 생성 보유하고 있는 정상 사용자들의 트레이스 백 정보를 이용하여 인증 과정을 수행한다.

정상 사용자란 트레이스 백 정보를 이용하여 구축해 놓은 사용자들의 접근 경로 정보와 일치하는 사용자들의 접근 정보를 의미한다.

그러므로 정상 사용자 접근으로 판정되면 서비스 접근을 허용하고, 일치하지 않을 경우 즉각 차단한다. 그렇지만 정상적인 트레이스 백 정보로 접근을 시도하지 않고, 다른 경로 정보를 이용하여 접근을 시도하는 경우에는 OTP를 발생시켜 인증과정을 수행한 후 접근 여부를 결정한다. 즉, 사용자 접근 트레이스 백 정보가 상이한 경우는 불법적인 사용자가 IP Spoofing을 이용하여 접근을 시도하는 경우와 정상적인 사용자 접근이지만 접근 위치가 일반적인 사용자 접근 경로를 이탈하여 접근하는 경우가 있다. 만일 정상 사용자가 트레이스 백 정보가 상이한 지역에서 접근을 시도하면, 이러한 경우에는 서비스 가용성을 향상시키기 위해 OTP를 이용하여 접근 경로 정보가 바뀌었다 하더라도, 서비스를 지속적으로 유지할 수 있도록 하였다.[10]



(그림 3) 제안모델 동작과정

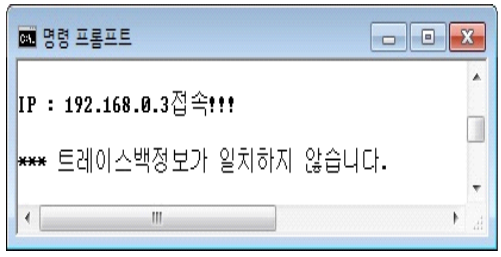
트레이스 백 정보에 대한 인증 과정을 통과하면 해당 서비스를 위한 어플리케이션 접근을 허용한다. 이때 접근 어플리케이션 등급이 1등급이면 OTP를 발생시켜 해당 어플리케이션이 서비스를 하는 자료 중 민감한 서비스 자료에 대해서는 암호화를 실시한다. 본 논문에서는 서비스 자료 중 범죄에 많이 이용되고 있는 '이름'과 '주민등록번호'에 대한 암호화를 실시하였다. 만일 2등급 자료 서비스를 수행하는 어플리케이션 사용 요청이 발생하면, 해당 접근 정보를 상호 협력체계에 있는 시스템들이, 상호 참조 가능한 접근 자료 데이터베이스에 등록을 해 둔다. 이는 향후 다른 2등급 어플리케이션 서비스 요청이 발생하여, 2등급 상호 서비스를 통하여 1등급 어플리케이션 서비스 자료에 준하는 민감한 자료로 전환이 될 수 있기 때문이다. 이러한 이유로 본 논문에서는 직원코드와 어플리케이션 등급 정보를 이용하여 서비스를 수행하는 자료 중 민감한 자료에 대하여 암호화를 수행한 후 서비스를 수행하도록 하였다.

이렇게 민원 서비스를 위한 모든 어플리케이션 접근 과정에 트레이스 백 정보와 OTP 인증 과정과, 민감한 자료들에 대하여 암호화를 수행한 후 서비스를 수행하고 있기 때문에, 중요한 자료들에 대한 관리 문제와 일반적인 자료에 대한 관리 및 서비스 가용성 문제를 개선 할 수 있다.

4. 실험 및 평가

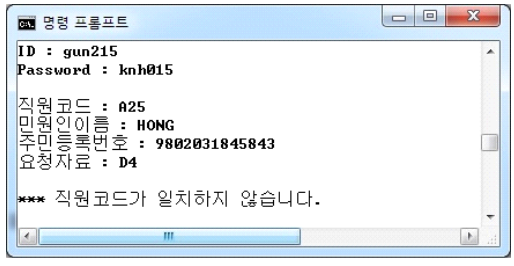
4.1 시뮬레이션 환경

본 논문에서 제안하고 있는 불법적인 정보 수집에 대한 방어 시스템 모델과 관련한 시뮬레이션 환경은 다음과 같다. 먼저 사용된 응용 소프트웨어는 jdk1.8.0_45, Eclipse 4.3.2 SR2, 구현언어는 Java를 사용하였다. 시뮬레이션을 위한 운영 체제는 Windows7 Professional K64비트이고, 시스템 사양은 8GB 메모리를 채택한 Core(TM)i5 2.67GHz System으로 구성하였다.



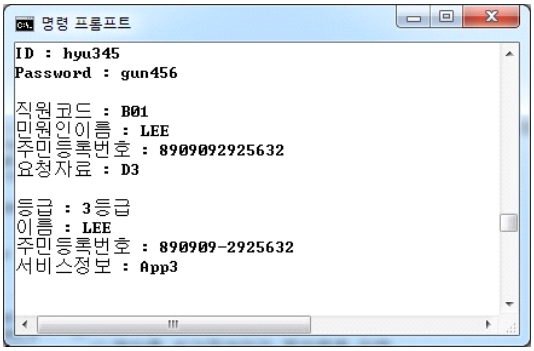
(그림 4) 서버에서 트레이스 백 정보 처리과정

(그림 4)의 경우는 사용자 접근이 발생하여 각 협력시스템에서 구축해 놓은 상호신뢰시스템의 트레이스 백 정보와 비교하여 일치하지 않을 경우 이를 차단하는 경우이다.



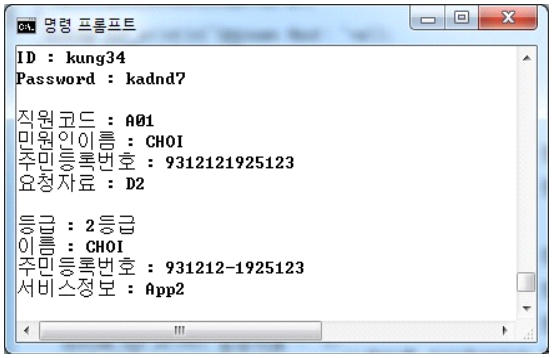
(그림 5) 직원코드가 일치하지 않은 경우

(그림 5)의 경우는 어플리케이션 사용 요청이 발생하여 <표 1>의 직원코드와 어플리케이션 목록을 비교하여 일치하지 않을 경우 이를 차단하는 과정이다.



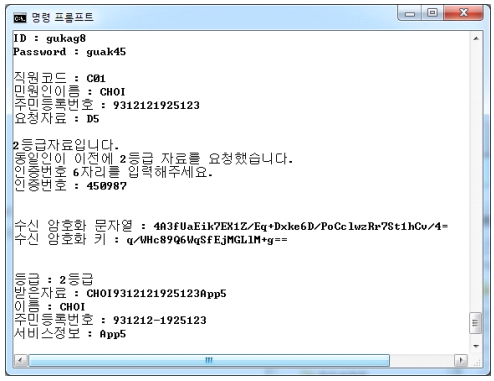
(그림 6) 3등급 자료 처리과정

(그림 6)은 빅데이터 환경에서 정상적인 사용자들이 일반적으로 서비스가 가능한 3등급 어플리케이션 서비스 자료들에 대한 결과이다.



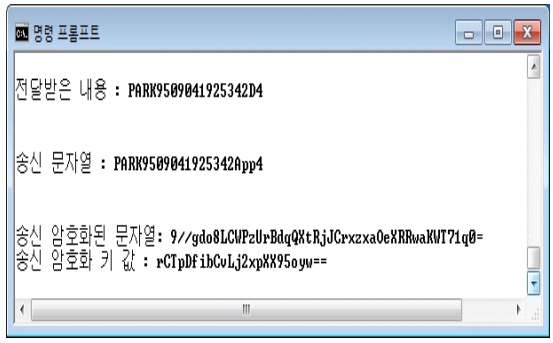
(그림 7) 2등급 자료 처리과정

(그림 7)은 빅데이터 환경에서 2등급 어플리케이션을 이용한 서비스 자료의 예이다. 이 자료는 향후 2등급 어플리케이션 서비스 자료 조합 유,무를 검사하기 위하여 상호 참조 가능한 데이터베이스에 등록을 해둔다.



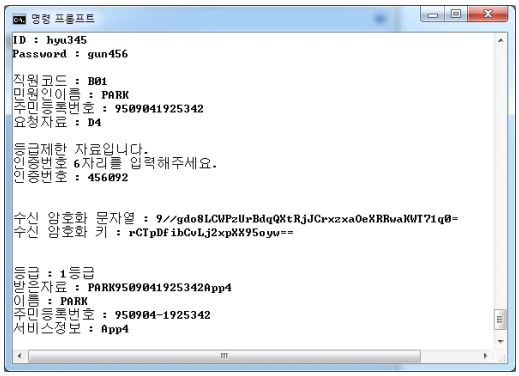
(그림 8) 2등급 자료가 조합이 발생한 경우

(그림 8)은 (그림 7)의 과정을 통하여 동일인에 대한 2등급 어플리케이션 서비스 요청이 추가로 발생했을 때 그 대응 과정을 보이는 것이다. 이 경우는 OTP를 이용한 2차 사용자 검증을 하게 된다. 그 다음 정상적인 사용자로 인증되면 해당 서비스 자료에 대하여 암호화를 수행한 후 이를 서비스 하게 된다.



(그림 9) 1등급 자료 서버에서 처리과정

(그림 9)는 민감한 내용을 포함하고 있는 자료에 대하여 암호화 서비스를 실시하는 1등급 어플리케이션 수행 과정의 결과이다.



(그림 10) 1등급 자료 서버에서 처리과정

(그림 10)은 (그림 9)의 과정을 통한 1등급 어플리케이션 서비스 요청이 발생했을 때 그 대응 과정을 보이는 것이다. 이 경우는 민감한 자료에 대한 서비스를 실시하는 것이므로 서비스 실시 전에 항상 암호화를 수행하도록 하였다. (그림 10)에서는 직원코드, 민원인 이름, 주민등록번호 중 주민등록번호가 민감한 자료이므로 이에 대한 암호화 과정을 수행하였고 그 결과를 나타내었다.

5. 결 론

본 논문은 현재 우리사회에 대두하고 있는 빅 데이터 환경에서 다양한 위치에 분산 관리되는 민원 서비스 센터의 서비스 과정에 대하여 안정성과 가용성을 고려한 모델을 설계한 것이다. 본 논문에서는 직원코드와 각 서비스 어플리케이션의 등급을 이용하여 보안 등급을 별도로 설계하고, 서비스를 수행하도록 하였다. 아울러 분산 저장 관리되는 자료들에 대한 어플리케이션 사용 조합이 발생할 경우, 이에 대한 보안 정책도 고려하였다. 그러므로 다양한 민원 서비스에 대하여 응용이 가능하리라고 본다. 향후 연구 과제로는 분산 저장되는 자료들에 대한 무선 환경 서비스까지 고려한 연구가 함께 이루어져야 할 것으로 보인다.

참고문헌

[1] J-K. Park, "A study on measures to active cultural contents service in big data age", Vol. 20, No. 1, pp. 324~334, Mar. 2014.

[2] D. Pansa and T. Chomsiri, "Architecture and Protocols for Secure LAN by Using a Software-level Certificate and Cancellation of ARP Protocol", Third 2008 International Conference on Convergence and Hybrid Information Technology, pp. 21~26, 2008.

[3] Steve Bellovin, Marcus Leech, Tom Taylor, "ICMP Traceback Message", IETF, draft-ietfitrace-04, Feb, 2003.

[4] 전정훈, "클라우드 컴퓨팅 서비스의 취약성과 대응 기술 동향에 관한 연구" 한국융합보안학회, Vol 13, No. 6, pp. 1239~1246, 2013. 4.

[5] Y-T. Mu, H-C. Baek, J-Y. Choi, W-C. Jeong, and S-B. Kim, "A Proposal of a Defence Model for the Abnormal Data Collection using Trace Back Information in Big Data Environments", Journal of the Korea Institute of Information and Communication Engineering, Vol. 10, No. 2, pp. 153~162, 2015.

[6] R-W. Huang, X-L. Gui, S. Yu, and W. Zhuang, "Privacy-Preserving Computable Encryption Scheme of Cloud Computing", Chinese Journal of Computers, Vol. 34, No. 12, pp. 2391~2402, 2011.

[7] J-K. Heo, "Web Application Authentication System using Encipherment and PKI", Journal of Information and Security, Vol. 8, No. 1, pp. 1~7, 2008

[8] 이경호, 김소정, 임종인, "전자정부와 프라이버시", 정보통신학회지, 제13권, 제3호, 2003. 6.

[9] 강푸름, 김귀남, "CCTV 영상자료 통합포털 구축 모델에 관한 연구", 한국융합보안학회, Vol 12, No. 2, pp. 43~51, 2012. 5.

[10] 허승표, 이대성, 김귀남, "모바일 환경에서 OTP 기술과 얼굴인식 기술을 이용한 사용자 인증 개선에 관한 연구", 한국융합보안학회, Vol 11, No. 3, pp. 75~84, 2011. 6.

[저 자 소 개]

김 명 희 (Myeong-hee Kim)

1992년 2월 경상대학교
국어국문학과 학사
2013년 2월 경상대학교
컴퓨터과학과 석사
2015년 2월 ~ 현재 : 경상대학교
컴퓨터과학과 박사 과정

email : kmh@inhaic.com

홍 석 원 (Suk Won Hong)

2003년 2월 경남과학기술대학교
컴퓨터공학과 학사
2006년 2월 경상대학교
컴퓨터과학과 석사
2011년 2월 경상대학교
컴퓨터과학과 박사
1999년 4월 ~ 현재 : 경남도립
거창대학

email : swhong@gc.ac.kr

백 현 철 (Hyun Chul Baek)

1988년 2월 경상대학교
전산통계학과 학사
1998년 8월 경상대학교
전산교육 석사
2003년 2월 경상대학교
컴퓨터과학과 박사
2013년 3월 ~ 현재 : 경남도립
남해대학 산학협력중점교수

email : dosi_gas@lycos.co.kr

박 재 흥 (Park Jae Heung)

1978년 2월 충북대학교
수학교육과 학사
1980년 9월 중앙대학교
전자계산학과 석사
1989년 8월 중앙대학교
전자계산학과 박사
1984년 4월 ~ 현재 : 경상대학교
교수

email : pjh@gnu.ac.kr