속성기반 암호를 이용한 스마트워크 환경에서의 데이터 접근제어

최슬기*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : skchoi@sch.ac.kr, jkwak@sch.ac.kr

Data Access Control using Attribute-Based Encryption in Smartwork Environment

Seul-Ki Choi*, Jin Kwak**
*ISAA Lab, Dept of Information Security Engineering, Soonchunhyang University.
**Dept of Information Security Engineering, Soonchunhyang University.

요 약

스마트워크는 언제 어디서나 편리하고 효율적으로 업무에 종사할 수 있도록 하는 미래지향적인 업무환경이다. 이미 국내·외 많은 국가 및 기업들이 스마트워크의 도입을 추진하고 있으며 이에 따라 기업 및 근로자 그리고 사회적인 측면에서 긍정적인 효과를 기대하고 있다. 하지만 다양한 환경에서 업무 데이터에 대한 접근이 가능하기 때문에 그에 따른 데이터 접근에 대한 보안 위협이 존재하다. 따라서 본 논문에서는 스마트워크 환경의 보안을 위하여 속성기반 암호 시스템을 이용하여 상황정보를 고려한 데이터 접근제어 기법을 제안한다.

1. 서론

최근 IT기술과 인터넷 기술의 발달로 인해 생활환경과 업무환경 등에 많은 변화를 가져왔다. 특히, 고성능의 연산 장치와 기억장치가 내장된 스마트 폰이나 태블릿과 같은 스마트 기기의 등장으로 인하여 사무실로만 한정되어 있었던 업무 공간의 제한이 없어졌으며, 언제 어디서나 편리하고 효율적으로 업무에 종사할 수 있도록 하는 미래지향적인 업무인 스마트워크가 가능하게 되었다.

스마트워크는 다양한 형태로 존재하는데 크게 스마트워크 센터 근무와 재택근무, 모바일 근무 등으로 구분할 수 있다. 따라서 스마트워크를 도입하는 조직 혹은 기관들의 성격과 근로자의 여건 등을 고려하여서 근무 형태를 정할 수가 있다.

Gartner에서 공개한 자료에 따르면 2015년에는 11조대 이상 스마트 폰이 판매될 것으로 예측되었다. 따라서 스마트 폰과 같은 스마트 기기들은 현재보다 더욱 많은 사람들에게 보급화가 되어가는 추세이고, 이로 인해 스마트워크의 가속화가 진행되고 있다.

스마트워크는 IT기술과 인터넷 기술 등을 융합하여 다양한 형태의 근무 환경을 제공하기 때문에 기존의 IT기술의 보안 취약점과 스마트워크 환경에서의 새로운 취약점이 발생할 수 있다. 특히 외부에서 내부 네트워크로 접근을 할 때 네트워크의 상태, 디바이스의 종류 및 성능 등의 상황정보를 고려하지 않은 채 사용자의 정보만을 기반으로 데이터의 접근 권한을 결정하게 되면 데이터 유출의 가능성이 존재한다. 따라서 본 논문에서는 속성기반 암호를 이용하여 사용자의 상황정보를 고려한 데이터 접근제어 기법을 제안한다.

본 논문의 구성은 2장에서는 관련연구로 스마트워크와 속성기반 암호에 대해서 분석한다. 3장에서는 기존 접근제어 방식의 위협을 분석하고, 4장에서는 상황정보를 고려한 접근제어 시스템을 제안한다. 5장에서는 제안 시스템에 대한 안전성을 분석하고 6장을 결론으로 끝을 맺는다.

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (No. 2012-0003208)

2. 관련연구

2.1 스마트워크

스마트워크는 종래의 사무실 개념을 탈피하여, 언제 어디서나 편리하고 효율적으로 업무에 종사할 수 있도록 하는 미래지향적인 업무환경이다[1]. 스마트워크의 유형으로는 스마트워크 센터 근무, 재택근무, 모바일 근무로 세 가지가 있다.

<표 1> 스마트워크 근무 형태

근무 형태	내 용
스마트워크 센터	지정된 사무실(스마트워크센터) 출근
재택근무	자택에서 사내 네트워크에 접속
모바일 근무	스마트기기 등을 이용한 업무 수행

❒ 스마트워크 센터

재택근무나 모바일 근무방식 보다는 비교적 보안성이 우수하고 본사와 유사한 수준의 사무환경을 제공한다. 또한 직접적인 가사 및 육아에서 벗어날 수 있기 때문에 업무 집중도를 향상 시킬 수 있는 장점을 가지고 있다.

❒ 재택근무의 경우

자택에서 직접 조직 및 기관의 네트워크에 접속하는 방식으로 별도의 사무공간이 필요하지 않으며 근무자의 출퇴근 시간 및 교통비, 그리고 본사의 운영 및 관리비용의 감소 효과를 얻을 수 있고, 업무와 가정 모두에 충실할 수 있다.

❒ 모바일 근무

스마트 폰이나 태블릿과 같은 스마트 기기 등을 이용하여 업무를 수행하는 근무형태로 대면 업무 및 이동이 많은 근무 환경에 유리하며 간편한 업무수행으로 시간을 절약하는 장점을 가지고 있다.

따라서, 스마트워크를 도입하는 조직 및 기관의 성격이나 근로자의 여건 등을 고려하여 다양한 형태로 스마트워크가 활용될 수 있다.

스마트워크의 도입은 일자리 창출, 저출산, 고령화 대책, 저탄소 녹색성장 등의 국가사회 경제 현안 문제들을 해결 가능하며 조기 은퇴자 및 현장 중심의 신속한 업무처리를 통하여 업무의 생산성을 향상시키는 등 기업과 근로자 그리고 사회적 측면에서 여러 가지 기대효과를 가져올 수 있다.

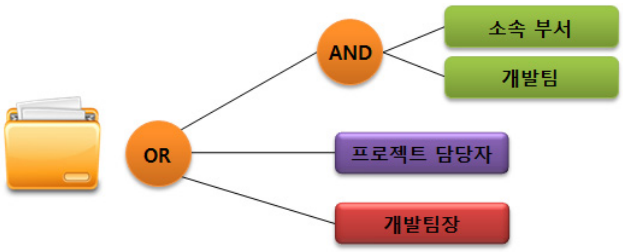
<표 2> 스마트워크의 기대효과

측 면	기 대 효 과
기업	- 업무 생산성 향상 및 고객만족도 증가 - 장기적 관점에서 사무 공간비용과 운영비 등의 절감 - 우수한 인재 확보 및 활용 - 조직의 전문성 강화
근로자	- 일과 삶의 균형 실현 - 생산성 및 효율성 향상 - 취업 기회의 확대
사회	- 사회간접 비용 절감 - 취업 소외계층의 취업 촉진 - 대도시 집중 완화 및 지방경제 활성화

2.2 속성기반 암호 (Attribute-based Encryption)

ABE의 개념은 2005년 Sahai와 Water에 의해 Fuzzy Identity-based Encryption(FIBE)로 처음 제안된 암호시스템으로 개체의 속성 정보의 집합과 속성의 접근구조를 바탕으로 암/복호화를 실시하는 방식이다. 여기서 접근구조란 주어진 속성 집합에 대해 접근을 허가하는지 아닌지를 결정하는 방법이다[2]. 사용자의 비밀키는 속성 집합과 관련되며 암호문은 속성 접근구조와 관련이 있다[3].

예를 들어, A 업체에서 보안 소프트웨어를 개발을 하고 있다고 가정할 때, 개발 중인 보안 소프트웨어의 데이터에 대한 접근을 개발팀 소속 직원이나 프로젝트 담당자 또는 개발팀장에게만 허용하고 싶다면 해당 데이터에 대한 접근구조를 아래 (그림 1)과 같이 만들어야 한다.



(그림 1) 접근구조

또한 직원의 비밀키는 소속 부서가 개발팀이거나 프로젝트 담당자이거나 개발팀장의 속성을 기반으로 만들어져야한다. 비밀키의 속성이 (그림 1)의 접근구조를 만족하면 직원은 데이터를 복호할 수 있다.

속성기반 암호시스템은 아래 4개의 알고리즘으로부터 구성된다.

① Setup(k) : 보안 파라미터 k(키 길이 등)를 입력하여 공개키 PK(Public Key)와 마스터키 MK(Master Key)를 출력하는 알고리즘.

② Encrypt(PK, AS, M) : 공개키 PK와 접근구조 AS(Access Structure), 그리고 메시지 M을 입력으로 하여 메시지 M에 대한 암호 메시지 C를 생성한다. 암호메시지 C는 메시지 M과 접근구조 AS를 포함하고 있는 메시지이다.

③ KeyGen(MK, S) : 마스터키 MK와 속성 집합 S을 입력하여 속성 집합 S에 대응하는 비밀키 SK(Secret Key)를 출력하는 알고리즘이다.

④ Decrypt(PK, SK, C) : 공개키 PK와 비밀키 SK, 그리고 암호메시지 C를 입력으로 평문 메시지 M을 복호한다.

3. 기존 접근제어 방식의 위협

스마트워크 환경에서 사용자는 여러 가지 근무형태로 조직 외부에서 조직 내부 네트워크로 접근을 할 수 있다. 각각의 근무형태마다 사용자가 이용하는 디바이스의 종류가 다양하고, 또한 각각의 디바이스 마다 성능도 모두 다르다. 그리고 사용자의 네트워크 환경도 사용자의 근무형태에 따라서 달라질 수 있으며, 똑같은 근무형태일지라도 네트워크 환경은 매번 달라질 수가 있다. 이처럼 매번 내부 네트워크에 접근할 때의 상황이 다를 수가 있기 때문

에, 상황 정보들을 고려하지 않은 채 사용자의 정보만으로 데이터에 대한 접근을 허락하는 기존 접근제어 방식은 데이터의 유출의 위협을 가지고 있다. 예를 들어 사용자 A의 소속 부서와 직급 등 사용자 정보만을 분석하여 내부 데이터에 대한 접근 권한을 허락하였다면, 이때에 사용자 A가 외부에서 내부 네트워크로 접근을 하는데, 암호화 통신을 적용하기에는 계산능력이 떨어지는 모바일 디바이스를 이용하게 되면 데이터의 유출이 발생할 수 있다. 또는 사용자 A가 사용하는 디바이스의 성능이 암호화 통신을 수행하기에 충분한 성능을 가지고 있더라도 누구나 패킷을 감청할 수 있는 공개AP(Access Point)를 이용하여 내부 데이터에 접근하는 경우에도 데이터의 유출이 일어날 수 있다.

4. 상황정보를 고려한 접근제어 시스템

본 논문에서는 속성기반 암호시스템을 사용하여 스마트워크 환경에서의 상황정보를 고려한 접근제어 시스템을 제안한다.

4.1 데이터 접근구조

각각의 데이터에 대한 접근구조를 결정할 때에는 사용자의 소속 부서와 직급, 역할 등의 사용자 정보뿐만 아니라 내부 네트워크로 접근하는 디바이스의 종류와 성능, 그리고 네트워크 상태 등의 상황 정보들도 접근구조의 속성으로 포함이 되어야 한다.

4.2 시스템 구성

제안하는 시스템의 구성 요소들은 아래와 같다.

- **사용자** : 스마트워크 환경을 이용하여 외부 장소에서 사내 네트워크로 접근하여 업무를 수행하는 사람으로서 인증 서버에 사용자 및 디바이스에 대한 인증 요청 기능을 수행한다.

- **사용자/디바이스 인증 서버** : 사내 네트워크로 접근하려는 사용자와 네트워크로 접근하는데 이용한 디바이스를 인증하는 서버이다. 사용자와 디바이스의 인증을 성공적으로 마친 후에는 인증에 사용된 사용자 정보와 상황 정보(사용자의 근무형태, 디바이스의 성능, 네트워크 상태 등)를 접근제어 센터에게 전송한다.

- **접근제어 센터** : Setup(k), KeyGen(MK, S) 알고리즘을 이용하여 사내 데이터를 암호화하기 위한 공개키 PK와 비밀키 SK를 계산하기 위한 마스터 키 MK를 생성한다. 그리고 각각의 데이터에 대한 접근구조 AS를 결정한다.

- **데이터 관리 서버** : 사용자의 데이터 접근에 대한 데이터 검색 및 전송 기능 등을 수행하며 접근제어 센터로부터 접근구조 AS와 공개키 PK를 전송받아 사내 데이터 M에 대하여 Encrypt(PK, AS, M) 알고리즘을 적용하여 사내 데이터를 암호화하여 데이터 저장소에 저장하는 기능을 수행한다.

- **데이터 저장소** : 데이터 관리 서버에 의해 암호화된 데이터를 저장하고 있는 저장소 역할을 수행한다.

4.3 데이터 암호화

사내에 저장된 데이터에 대한 접근 과정을 수행하기 전에 모든 데이터들의 암호화 과정이 우선적으로 이루어져있어야 한다. 데이터의 암호화 과정은 아래와 같다.

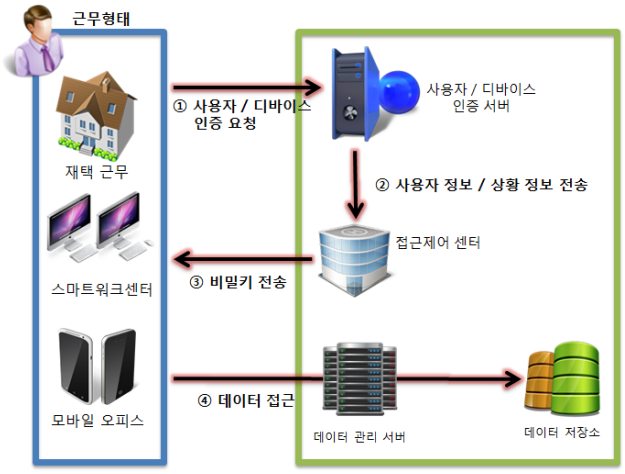
① 접근제어 센터는 Setup(k) 알고리즘을 이용하여 공개키 PK와 마스터키 MK를 생성한 뒤, 이어서 암호화할 데이터의 유형과 사용 목적에 알맞은 접근구조 AS를 생성하여 데이터 관리 서버에게 PK와 AT를 전송한다.

② 데이터 관리 서버는 접근제어 센터로부터 전송받은 공개키 PK와 접근구조 AS를 이용하여 암호화할 데이터 M에 암호화 알고리즘 Encrypt(PK, AS, M)을 적용하여 암호화된 데이터 C를 얻어낸다.

③ 데이터 관리 서버로부터 생성된 C를 데이터 저장소에 저장한다.

4.4 데이터 접근 시나리오

아래 (그림 2)는 스마트워크 근무자가 외부장소(재택근무, 스마트워크 센터, 모바일 근무 등)에서 업무를 지속적으로 수행하기 위해서 사내 네트워크로 접근하여 업무를 위한 데이터에 접근하기까지의 과정을 나타낸 그림이다.



(그림 2) 데이터 접근 시나리오

① 외부장소에 있는 사용자가 사내의 인증서버에 사용자 및 네트워크 접근에 사용된 디바이스에 대한 인증을 요청한다.

② 사용자/디바이스 인증 서버는 사용자 및 디바이스 인증 과정에서 얻은 사용자 정보(소속부서, 직급, 역할 등)와 디바이스 정보(종류, 성능 등)를 통하여 사용자의 근무 환경에 대한 상황 정보(근무 유형, 네트워크 상태, 디바이스 성능)을 생성하고 사용자 정보와 상황 정보를 접근제어 센터에 전송한다.

③ 사용자/디바이스 인증 서버로부터 전송받은 사용자 정보와 상황 정보를 이용하여 현재 사용자에 대한 속성 S를 결정한다. 사용자에 대한 속성 S와 Setup(k) 알고리즘을 통하여 생성한 마스터키 MK를 비밀키 생성 알고리즘 KeyGen(MK, S)에 적용하여 비밀키 SK를 생성하고 사용자에게 전송한다.

④ 접근제어 센터로부터 전송받은 비밀키 SK와 공개키 PK를 이용하여 암호화된 데이터에 Decrypt(SK, PK, C) 알고리즘을 적용하여 데이터를 복호한다.

5. 안전성 분석

5.1 데이터 접근제어

스마트워크 사용자는 근무형태와 사용하는 디바이스에 따라서 다양한 방법으로 사내 네트워크에 접근을 할 수 있다. 따라서 사내 네트워크에 접근하려는 사용자의 상황 정보를 고려하지 않은 채 사용자의 정보만을 고려하여 데이터에 대한 접근 권한을 결정하게 된다면 내부 데이터의 유출이 일어날 수 있다. 본 논문에서 제안한 접근 제어 기법은 데이터에 대한 접근구조에 상황 정보까지 고려할 수 있는 속성들을 추가하였기 때문에 기존의 접근 제어 방식보다 안전성을 높일 수 있다.

5.2 공모 공격

속성기반 암호화 방식은 공모 공격에 대한 안전하다는 중요한 보안 특성을 갖고 있다. 공모 공격이란 둘이상의 사용자들이 그들의 속성집합을 조합하여 그들의 복호 권한을 확장시키는 공격이다. 예를 들어 사용자 A의 비밀키는 속성 집합 S_A=(A, C)로 구성되어 있고, 사용자 B의 비밀키는 속성 집합 S_B=(B, D)로 구성되어 있을 경우, 접근구조 AS=(A∧B)로 구성된 암호문을 복호하기 위하여 사용자 A와 사용자 B의 비밀키를 조합하여서 $S_A \cup S_B$=(A, B, C, D)의 속성 집합으로 구성된 비밀키를 생성하는 것이다.

속성기반 암호화 방식의 KeyGen 알고리즘의 상세과정에는 각 사용자의 고유 식별자를 임의의 난수로 생성하여 비밀키 생성과정에 포함이 된다. 따라서 본 논문에서 제안한 시스템의 구성요소인 접근제어 센터가 임의의 난수로 선택한 사용자의 고유 식별자를 각 사용자가 알아낼 수 없기 때문에 비밀키를 조합하는 공모 공격에 대해서 안전성을 갖는다.

6. 결론

스마트워크 환경은 다양한 환경에서 내부 네트워크로 접근이 가능하기 때문에 사용하는 디바이스의 종류와 성능, 네트워크 환경 등을 고려하지 않은 채 사용자 정보만으로 접근 제어를 하게 되면 데이터 유출이 일어날 수 있다. 따라서 본 논문에서는 속성기반 암호를 적용하여 상황 정보까지 고려한 데이터 접근제어 방법은 제안하였다.

본 논문에서 제안한 접근제어 방법을 이용하여 스마트워크에서의 데이터 유출 방지에 도움이 될 것으로 기대한다. 또한 지속적으로 발전하고 있는 스마트워크 환경에서 발생 가능한 새로운 보안 취약점에 대해서 연구를 하고 발견된 보안 취약점에 대비할 수 있는 기술들에 대한 연구가 필요하다.

참고문헌

[1] 한국전자통신연구원, "스마트워크 표준화 동향", 2011
[2] 박광용, 송유진, "속성기반 암호기술", 정보보호학회지, 제20권 제2호, 2010
[3] 송유진, 도정민, "속성기반 암호화를 이용한 원격 헬스케어 모니터링 시스템", 정보처리학회논문지, 제19권 제1호, 2012
[4] 이민혜, 이준기, "스마트워크 연구에 대한 고찰과 향후 연구 주제", 한국정보화진흥원 정보화정책 제18권 제2호, 2011
[5] 이형창, 이정현, 손기욱, "스마트워크 보안 위협과 대책", 한국정보보호학회지, 제21권 제3호, 2011
[6] 정종민, 권태경, "속성기반 암호기술을 이용한 컨텐츠 네트워크 보안 표준기술", 한국정보통신기술협회 제6회 정보통신 표준화 우수논문집, 2010
[7] 임광현, 이동진, 김진혁, "스마트워크 연구경향분석", 한국정보화진흥원 정보화정책 제17권 제4호, 2010