http://dx.doi.org/10.14400/JDPM.2013.11.12.407

클라우드 환경에서의 통합 보안관제 모델 연구

변연상*, 곽진**
순천향대학교 정보보호학과 정보보호응용및보증연구실*,
순천향대학교 정보보호학과**

A Study on Integration Security Management Model in Cloud Environment

Yun Sang Byun*, Jin Kwak**
ISAA Lab. Department of Information Security Engineering Soonchunhyang University*
Dept of Information Security Engineering, Soonchunhyang University**

요 약 최근 다양한 IT 서비스 및 컴퓨팅 자원을 인터넷 기반으로 제공받을 수 있는 클라우드 환경에 대한 사용자들의 관심이 증가하고 있으며, 이에 따라 클라우드 환경의 보안에 대한 관심 또한 증가하고 있다. 클라우드 환경은 다양한 사용자들에게 적절한 서비스를 제공하기 위해 막대한 양의 IT 자원 및 서비스들을 클라우드 상에 저장하고 사용자의 요구에 따라 제공하기 때문에 저장된 데이터 및 자원들에 대한 무결성, 불법 유출, 위·변조와 같은 보안 사고를 예방하고 신속하게 처리할 수 있는 능력이 요구된다. 그러나 기존에 개발된 다양한 솔루션이나 연구결과들은 클라우드 환경을 고려하지 않고 개발 및 연구되었기 때문에 클라우드 환경에 접목시키기에는 다소 무리가 있다. 따라서 이러한 문제를 해결하기 위해 본 논문에서는 클라우드 환경에서 발생할 수 있는 다양한 보안 사고를 사전에 방지하고, 발생 시 신속하게 대응할 수 있는 유·무선 통합 보안관제 모델을 제안한다.

주제어 : 클라우드, 보안관제, 통합 보안관제, 클라우드 환경 보안관제, 보안관제 프레임워크

Abstract Recently, Interest variety of IT services and computing resources are increasing. As a result, the interest in the security of cloud environments is also increasing. Cloud environment is stored that to provide services to a large amount of IT resources on the Cloud. Therefore, Cloud is integrity of the stored data and resources that such as data leakage, forgery, etc. security incidents that the ability to quickly process is required. However, the existing developed various solutions or studies without considering their cloud environment for development and research to graft in a cloud environment because it has been difficult. Therefore, we proposed wire-wireless integrated Security management Model in cloud environment.

Key Words : Cloud Computing, Integration Security management, Security Management, Cloud Environment Security management, Security management Framework

* 이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-010886).
* 이 논문은 순천향대학교의 지원을 받아 수행된 연구임
* 이 논문은 2013학년도 순천향대학교 교수 연구년제에 의하여 연구하였음.
Received 20 November 2013, Revised 18 December 2013
Accepted 20 December 2013
Corresponding Author: Jin Kwak(Soonchunhyang University)
Email: jkwak@sch.ac.kr

ISSN: 1738-1916

1. 서론

최근 다양한 IT기술들에 대한 개발 및 연구가 활발하게 진행됨에 따라 하드웨어 또는 각종 소프트웨어와 같은 다양한 컴퓨팅 자원을 구매, 설치하지 않고 필요할 때만 사용하고, 그에 따른 요금을 지불하는 형태의 컴퓨팅 서비스인 클라우드 컴퓨팅에 대한 관심이 증가하고 있다. 많은 IT 기술들 중에서도 클라우드 컴퓨팅이 널리 상용화되고 인기가 있는 이유는 서로 다른 위치에 존재하는 무형의 형태로 존재하고 있는 하드웨어, 소프트웨어와 같은 컴퓨팅 자원들을 가상화 기술을 통해 사용가능하기 때문이다[1,2,3,4].

클라우드 환경에서는 다양한 자료들이 외부 서버에 저장되어 관리되고 있기 때문에 보다 안전하게 각종 데이터 및 자원들을 관리 및 보관할 수 있으며, 저장 공간에 대한 환경적인 문제 또한 해결할 수 있다.

클라우드 환경은 언제 어디서든 시간과 장소에 구애받지 않고 자신에게 필요한 각종 데이터 또는 컴퓨팅 자원 등을 이용하거나 열람 및 수정할 수 있는 장점이 있다. 그러나 해당 클라우드 서버자체가 공격받거나 취약점에 노출될 될 경우, 개인정보가 유출되거나 저장된 데이터 및 자원들의 무결성을 제공할 수 없으며, 서버의 장애가 발생함에 따라 저장된 데이터 및 자원의 이용이 불가능하게 될 가능성이 존재한다. 또한 클라우드 환경에 저장 및 관리되고 있는 데이터의 경우 보안상 취약하기 때문에 해당 데이터를 암호화하여 관리하여도 데이터는 클라우드 서버에 저장되어 있기 때문에 다양한 사용자 디바이스에 제공하는 과정에서 해당 데이터 및 자원들이 유출될 가능성이 있다. 또한 클라우드 환경에서 사용되고 있는 플랫폼의 경우 공격의 용이함과 취약점이 쉽게 발견되고 있지만 그에 따른 보호 기법이나 관련 연구가 부족한 실정이다[3,4].

본 논문에서는 다양한 클라우드 환경에 접근하는 수많은 사용자들과 각종 디바이스의 접근부터 서버에 저장되어 있는 다양한 데이터 및 자원들을 관리하며, 해당 클라우드 서버의 취약점을 통해 보안사고 발생 시 빠르게 대응하고, 안전하게 서비스를 제공하기 위한 보안관제 모델을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 클라우드와 보안관제에 대한 분석을 진행하고, 3장에서는 클라우드 환경에서 발생할 수 있는 취약점 및 요구사항에 대해서 분석한다. 4장에서는 클라우드 환경에서의 보안관제 모델을 제안한다. 5장에서는 도입효과를 분석하고, 마지막으로 6장에서 결론으로 마무리 짓는다.

2. 관련연구

2.1 클라우드

클라우드 환경은 언제 어디서나 시·공간에 제약 없이 서버에 저장된 데이터 또는 컴퓨팅 자원을 사용자의 필요성에 따라 네트워크를 통해 다양한 방식으로 서비스를 제공받는 기술을 의미한다[1,2]. 즉, 클라우드는 하드웨어나 소프트웨어, 스토리지 또는 네트워크 등과 같이 사용자가 사용 가능한 대부분의 컴퓨팅 자원들을 구매 또는 설치하지 않고, 필요한 만큼 서비스를 요청하여 제공받아 사용하고 그에 따른 사용요금을 지불하는 형식으로 서비스를 제공하고 있다.

클라우드 서비스는 종류에 따라 크게 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service) 등으로 구분되며, 최근 서비스 제공업체의 상황에 따라 다양한 형태의 서비스를 제공하고 있다[4,5,6]. IaaS는 서버나 스토리지 등과 같은 인프라 자원을 제공하는 서비스로, 아마존의 AWS와 Rackspace 등이 대표적인 예다. PaaS는 표준화 된 플랫폼을 서비스로 제공하는 서비스로 Google의 AppEngine과 Microsoft의 Asure가 있다. SaaS(Software as a Service)는 사용자가 이용하는 웹 브라우저를 기반으로 소프트웨어를 제공하는 서비스이다. 대표적인 예로 Google의 Gmail과 Salesforce.com 등 이 있다

또한 클라우드 환경은 배치하는 형식에 따라 사설 클라우드(Private Cloud)와 공공 클라우드(Public Cloud)로 구분할 수 있다. 사설 클라우드의 경우 특정 개인 또는 기업 고객만을 대상으로 한 클라우드 서비스로 기업에서 자체적으로 환경에 적합한 사설 클라우드를 구축하여 사용하기 때문에 전반적인 기반시설에 대해 완전한 통제가 가능하고, 데이터에 대한 보안성을 유지하기 용이하다는 장점이 있다. 공공 클라우드는 사설 클라우드와는 다르게 불특정 다수의 개인이나 기업을 위한 클라우드 서비스이다. 공공 클라우드의 경우 제공되는 모든 서비스를

내부로부터 외부에서 수신할 수 있기 때문에 관리가 쉬울 뿐만 아니라 유지 보수비용에 대한 절감 효과를 기대할 수 있다. 그러나 해당 데이터가 외부에 존재하기 때문에 기반 시설에 대한 통제권 확보가 불가능하며, 서비스 중단이 발생할 경우 개인이나 기업의 업무가 마비될 수 있다[7,8,9].

[Fig. 1] Cloud Computing Environment

2.2 보안관제

보안관제는 관제 대상기관의 정보 기술 및 다양한 IT 자원을 해킹, 바이러스 등과 같은 여러 사이버 공격으로부터 보호하기 위해 각종 보안 이벤트 및 시스템 로그 등을 관제 센터에서 실시간으로 모니터링을 수행하고, 분석을 통해 해당 문제점에 대하여 대응하는 보안 업무를 나타낸다.

저장된 중요한 정보 자산의 관리 및 보안은 전문적인 집단에서 수행하고, 대상기관의 경우 해당 업무를 중점적으로 수행할 수 있다는 장점을 가진 보안 서비스이다. 보안관제의 경우 기존의 '정보공유분석센터'와 유사한 형태로 업무의 분야를 구분하여, 해당 분야에 대한 해킹, 바이러스 등과 같은 사이버 공격 및 다양한 정보의 침해사고 등에 대해 대응하기 위한 방식이다. 또한 취약점 및 침해 요소 등을 분석하고 대응방안을 모색하여 대상기관에 정보를 제공하거나, 보안사고가 발생할 경우 실시간 모니터링을 통해 빠른 대응을 수행하는 점에서 유사하다. 추가적으로 분야별 여건을 고려, 침해사고 대응체계 구성 및 운영, 기반 시설 보호, 정보보호 관련 교육 등 다양한 부가 서비스 제공을 통해 대상기관의 정보보호 관련 분야를 전반적으로 다루기 때문에 별도의 전문조직 운영을 위한 비용을 절감할 수 있으며, 솔루션 구입이나 기술 확보 등과 같은 다양한 요소들에 대한 문제를 해결할 수 있다[10,11].

보안관제의 구성요소는 크게 3가지로 네트워크나 시스템에 설치된 에이전트, 정보수집 서버, 관제용 시스템으로 구성된다. 먼저 에이전트 의 경우 각종 보안 장비와 서버, 네트워크 등에 설치하여 해당 시스템에 적합한 설정에 따라 로그 정보를 실시간으로 전송하여 관제센터에서 각종 로그를 손쉽게 분석할 수 있도록 정보를 제공해주는 역할을 수행한다. 다음으로 정보수집 서버는 각각의 에이전트에서 보내진 각종 정보를 수집 및 처리하여 데이터베이스에 저장하는 역할을 수행한다. 이때 에이전트에 대한 확인 작업을 통해 모니터링과정 및 분석과정에 요구되는 각종 리포팅 소스를 제공한다. 끝으로 통합관제용 시스템은 각종 이벤트의 로그에 대한 분석을 수행하여, 다양한 정보를 종합 및 상황 분석을 통하여 관제 인원들을 지원하는 역할을 수행한다[9].

보안관제는 유형에 따라 크게 원격관제, 파견관제 및 자체관제 3가지로 분류된다. 먼저 원격관제의 경우 관제 업체가 보안관제에 필요한 관제시스템을 스스로 구비하여 대상기관의 침입차단시스템 등 보안장비 중심의 보안 이벤트에 대하여 상시 모니터링 과정을 수행하고 만약 침해사고가 발생할 경우 신속하게 대응 조치하는 서비스이다. 파견관제는 대상기관이 직접 자체적으로 보안관제 시스템을 구축하여 관제 업체로부터 전문 인력만 파견을 받아 관제 업무를 수행하는 형태이다. 끝으로 자체관제의 경우 보안관제시스템의 구축 및 관제 전문 인력을 양성하여 자체적으로 운영 및 관리하는 관제 형태이다[10].

3. 취약점 분석 및 요구사항분석

3.1 취약점 분석

3.1.1 물리적 보안제어 부족

클라우드를 이용하는 사용자들은 집 또는 회사, 외부 공간 등과 같은 다양한 장소에서 디바이스를 이용하여

서비스를 제공 받는다. 이러한 경우 디바이스들의 이동성 확보와 사용자들의 편리성을 확보할 수 있다. 그러나 디바이스 분실 및 도난과 같은 위협에 노출될 수 있으며, 그로인한 디바이스 내에 저장된 데이터의 유출 및 위·변조가 발생할 가능성이 존재한다. 사용자들이 이용하는 각종 디바이스들은 항상 소지하고 있을지라도 외부공간에서 숄더 스니핑(Shoulder Sniffing)을 통해 노출되거나 화면에 출력된 데이터들이 보이는 것과 같은 물리적인 보안 위협에 노출될 수 있다[12,13,14,15].

3.1.2 취약한 통신망 사용

클라우드 서비스를 제공받기 위해 원격접속을 수행하는 사용자들은 대부분 인터넷을 통해 이루어지고 있으며, 일반적으로 외부에서 대다수의 사용자들이 사용하는 외부통신망은 보안에 대한 통제가 사실상 불가능하다. 이러한 외부통신망의 경우, 도청에 취약하며 원격접속을 수행하는 동안 송·수신되는 데이터들은 민감한 정보를 포함하고 있을 수 있다. 또한 해당 데이터가 도청이 될 경우 위·변조의 위험에 노출될 수 있다. 또한 중간자 공격(Man-In-The-Middle-Attack)으로 인하여 송·수신되는 데이터를 탈취하여 변형할 수 있다[13].

취약한 통신망을 많은 사용자들이 사용함으로써 발생할 수 있는 위협들은 데이터의 무결성과 기밀성을 유지함과 동시에 사용자와 서버간의 상호인증을 통하여 완화시키는 것이 가능하지만 완전하게 제거하는 것은 불가능하다.

3.1.3 내부자원 접근

클라우드 서비스는 수많은 사용자들이 외부에서 사용자들이 디바이스들을 사용하여 클라우드에 저장된 데이터에 접근하게 된다. 다양한 환경에서 신뢰되지 않은 디바이스를 통해 내부자원에 접근할 경우, 데이터의 위·변조 될 가능성이 증가할 뿐만 아니라 클라우드 서버에 바이러스와 같은 악성코드를 전파시키는 것 또한 가능하게 된다. 따라서 적법한 사용자/디바이스를 판별하여 사용자의 접근 및 데이터 접근을 제어할 수 있어야 한다[13].

3.2 요구사항분석

3.2.1 기술적 요구사항

클라우드 환경은 다양한 IT기술이 가상화 기술을 통해 분산된 시스템으로 구성되어 있다. 이러한 환경에서 보안 시스템을 운영하는 것은 어려운 일이다. 이러한 문제를 해결하기 위해 보안관제와 같은 사고 대응 및 예방 시스템이 필요하다. 또한 점차 고도화되는 침해사고들 뿐만 아니라 이로 인해 발생할 수 있는 2차 피해를 방지하기 위해 신속하고 전문화된 대응 체계의 구축이 필요하다. 클라우드 서버 내에서 보안 관제를 실시함으로써 보다 능동적이며 체계적으로 취약점에 대응할 수 있는 시스템을 구축하여 각종 침해사고를 사전에 예방할 수 있는 시스템이 요구된다[1,2].

3.2.2 환경적 요구사항

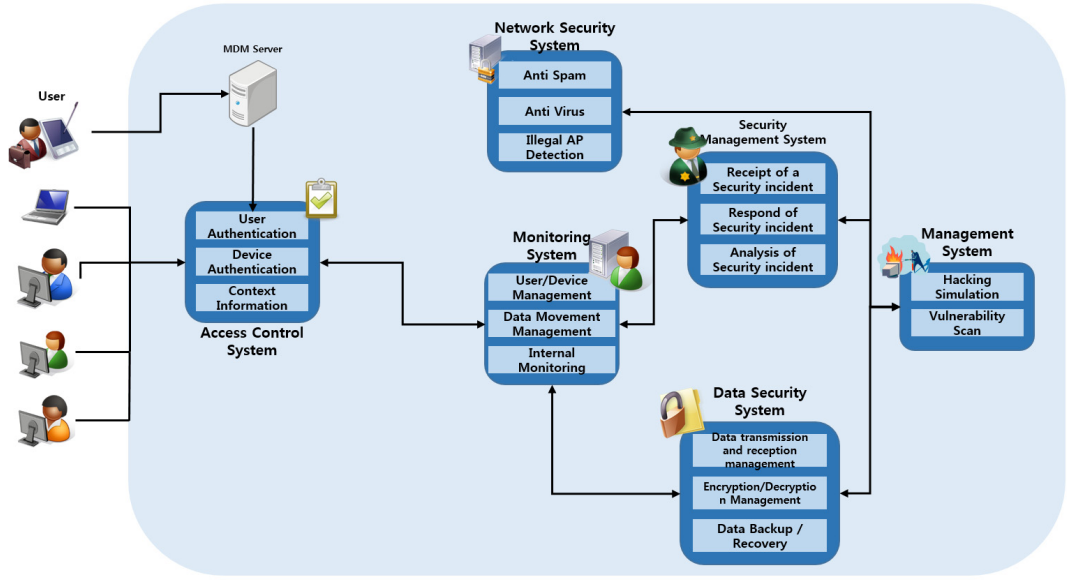
IT기술의 발전으로 인해 사용자들의 보안 사고에 대한 인식이 증가하고 있다. 그러나 보안 사고에 대한 대응 체계가 확립되지 않았으며, 클라우드 서버를 관리해줄 보안시설이 존재하지 않는 경우가 많다. 이로 인해 해킹, 데이터 유출과 같은 1차 피해뿐만 아니라 개인정보의 악용과 같은 2차 피해가 발생할 가능성이 증가하고 있다. 이러한 문제점을 해결하기 위해 보안 사고에 대한 대응 체계와 보안시설의 마련에 대한 필요성이 증가하고 있다.

또한 최근 들어 침해사고가 지속적으로 증가하고 있으며 점차적으로 지능화, 고도화됨에 따라 일괄적인 대응이 어려운 실정이다. 이에 따라 점차 진화하는 공격에 대응하고, 복합적인 문제를 해결할 수 있는 시스템의 구축이 필요하다[1,2,3].

3.2.3 운영적 요구사항

클라우드 환경은 다양한 IT기술의 융합으로 인해 시스템이 점차 복잡화되고 있으며, 범위가 점차적으로 대형화가 진행되고 있기 때문에 저장된 자원 및 시스템의 보안 관리 및 유지하기 위한 담당자의 업무량이 증가하고 있다. 또한 막대한 양의 데이터들을 안전하고 체계적으로 관리하기 위한 관리 기법이 필요하다. 이러한 문제점을 해결하기 위해서는 자동화 및 체계적이고 복합적인 보안관리 시스템의 구축이 요구되고 있다.

또한 다양한 솔루션을 기반으로 보안 업무를 수행하기 때문에 발생할 수 있는 비용적 측면의 문제도 고려사항이다. 이러한 종합적인 문제를 해결을 위해 통합된 관리 체계가 요구되고 있다[2],[3].



[Fig. 2] Security Management Model

4. 제안기법

클라우드 서비스는 수많은 사용자들이 언제 어디서나 동시 다발적으로 이용 가능한 서비스로 만약 인증과정을 수행하지 않고 사용자의 접근이 허가된다면 해당 사용자에 의해 악성코드가 유포되거나 서버 내에 악성 파일을 업로드 시키는 경우가 발생할 수 있다. 또한 서버 내에 저장된 데이터의 위·변조 또는 기밀 데이터의 유출이 발생할 가능성이 존재한다.

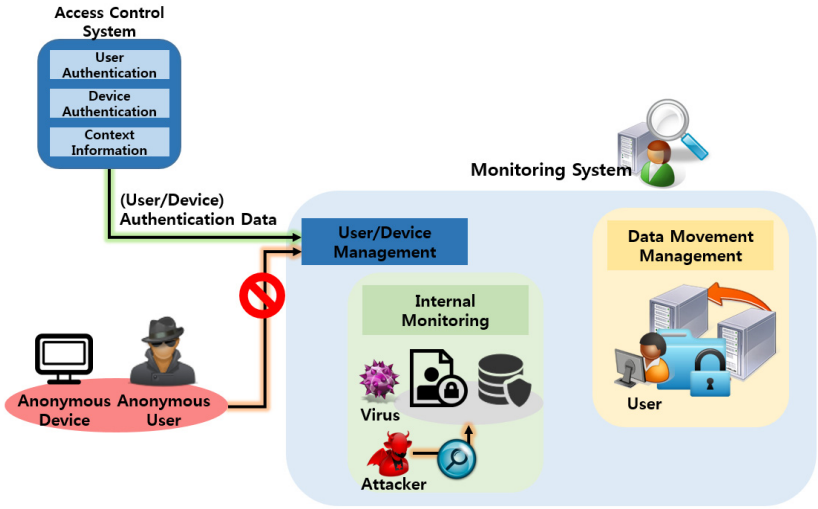
본 절에서는 클라우드 환경에서 유·무선 통합 보안관제 모델을 제안한다. 제안 기법은 크게 모니터링 시스템, 자동화 관제 시스템, 네트워크 보안 시스템, 데이터 보안 시스템, 관리 시스템 및 접근제어 시스템으로 구성되어 있으며, 그 외 하위 모듈들이 보안 관제 시스템을 구성한다. 제안하는 보안관제 모델은 [Fig. 2]와 같다.

4.1 모니터링 시스템

모니터링 시스템은 클라우드 서버 내에서 실시간으로 이용현황 및 보안 이벤트, 사용자/디바이스 등을 관리하는 시스템으로 사용자/디바이스 관리 모듈과 데이터 이동 관리 모듈, 서버 내 실시간 모니터링 모듈로 구성되어 있다.

사용자 디바이스 관리 모듈은 클라우드 서버에 접근하는 수많은 사용자의 관리 및 사용자가 이용하는 디바이스를 관리하는 모듈로, 접근제어 시스템과 연계하여 사용자 및 디바이스의 적법성을 확인 및 관리한다. 만약 이상 징후가 탐지될 경우 관제 시스템으로 해당 로그를 전송하여 대응 및 분석을 통해 이상 징후를 해결할 수 있도록 조치를 취한다.

데이터 이동 관리 모듈은 클라우드 서버 내에 저장된 수많은 데이터의 이동 관리를 전담하는 모듈이다. 데이터의 이동 관리를 위해 접근제어 시스템의 상황 정보 모듈과 연계하여 해당 사용자의 상황에 따른 데이터 접근 권한, 처리능력 등에 대한 정보를 수신하여 불필요하거나 부적합한 데이터의 이동을 차단 및 관리한다. 서버에 저장된 각종 데이터들은 특정 코드 또는 해쉬값을 함께 기록하여 데이터의 이동과정 및 경로를 관리 하게 된다. 실시간 모니터링 모듈은 사용자들이 업로드 한 데이터의 위·변조가 발생하거나, 저장된 데이터에서 악성코드가 활동하는 경우 등 클라우드 서버 내에서 실시간으로 발생하는 보안 이벤트들을 탐지 및 관리하고 대응할 수 있는 모듈이다. 또한 서버에 접속한 사용자가 불법 행동을 하거나 불법 파일의 업로드 및 다운로드를 탐지하고 사전에 차단한다. 모니터링 시스템의 모듈을 도식화하면



[Fig. 3] Monitoring System Module

다음 [Fig. 3]과 같다.

4.2 자동화 관제 시스템

자동화 관제 시스템은 전반적인 관제 시스템을 통해 수집되는 이벤트들을 수신하여 클라우드 서버를 관리한다. 이벤트가 발생할 경우 발생 시점부터 발생 상황, 피해 정도를 수집하여 분석을 통해 해당 상황에 적절한 대응책을 자동을 수행한다. 또한 수집 및 분석된 데이터를 정리하여 관리자가 이해하기 쉽도록 도움을 준다. 만약 바이러스가 클라우드 서버에 저장된 파일에 감염되었을 경우, 해당 이벤트를 접수하고 분석을 통해 네트워크 보안 시스템의 안티 바이러스 모듈을 실행시켜 감염된 파일을 격리/치료를 수행하고, 함께 저장되어 있던 파일의 감염 여부를 확인한다.

자동화 관제 시스템은 모든 구성요소들과 연계하여 보안 이벤트 발생 및 긴급 상황이 발생할 경우 해당 상황에서 가장 적합한 대응책을 제안하여 문제를 해결한다. 클라우드 상에서 위협을 탐지할 경우 보안 위협에 대응할 수 있는 모듈을 호출하여 해당 보안 위협을 차단한다. 예를 들어, 클라우드 상에서 악성코드에 감염된 데이터가 탐지될 경우, 네트워크 보안 시스템의 안티 바이러스 모듈을 호출하여 해당 데이터를 진단하여, 치료, 격리 및 삭제 등의 대응을 수행한다. 데이터를 삭제 하였을 경우, 해당 데이터의 소유주 및 사용자에게 사고 내용에 대한 보고서 및 안내문을 공지하여 추가적인 사고를 방지한다.

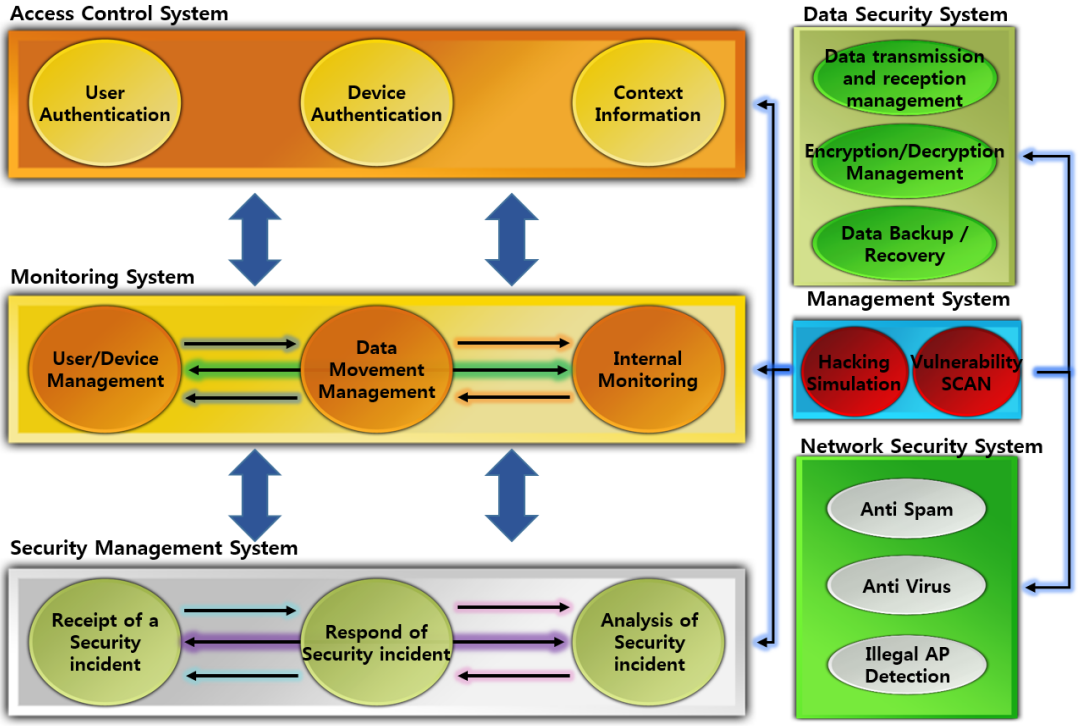
4.3 네트워크 보안 시스템

네트워크 보안 시스템은 클라우드 시스템 내에서 발생하는 각종 보안 사고에 대해서 대응하기 위한 시스템으로 크게 안티 바이러스 모듈, 불법 AP 탐지 모듈로 구성되어 있다.

안티 바이러스 모듈은 기존에 정의된 바이러스의 정의 및 패턴을 분석하여 바이러스 DB에 저장된 데이터와 비교를 통해 바이러스를 탐지한다. 또한 데이터 내부의 코드 일부가 바이러스 정의와 일치할 경우 바이러스를 제거하고 파일의 위험성 테스트를 진행한다. 테스트를 통과하지 못할 경우 파일을 차단하고, 삭제한다.

불법 AP 탐지 모듈은 비인가 된 무선 AP를 통하여 클라우드 서버에 접속할 경우 이를 감지하여 패킷 전송을 차단하는 감지 모듈이다. 불법 AP 탐지를 통해 공개된 AP 사용자의 접근을 제한한다.

네트워크 보안 시스템은 데이터 보안 시스템과 연계하여 내부에 저장된 데이터의 이동 및 전송 과정을 감지 과정을 수행하여하여 비 인가된 AP로 접근한 사용자로부터 클라우드에 저장된 데이터가 외부로 유출되는 것을 탐지하여 차단하고 로그를 생성한다. 또한 디바이스의 캡처 기능을 이용하여 데이터가 유출되는 것을 방지한다.



[Fig. 4] The processing of each system module

4.4 데이터 보안 시스템

데이터 보안 시스템은 클라우드에 저장된 데이터들은 전무 암호화를 통하여 특정 사용자 또는 권한을 획득한 사용자들에게만 접근이 가능하도록 하며, 비 인가된 사용자는 해당 데이터에 접근이 불가능하도록 관리를 수행한다.

데이터 보안 시스템은 데이터 관리 서버를 기반으로 모든 데이터의 이동, 복사 등을 관리하게 된다. 또한 클라우드에 저장되는 데이터는 사소한 데이터부터 각종 개인정보, 중요 데이터 등이 될 수 있기 때문에 데이터의 암호화를 수행하여 저장한다. 이 후 암·복호화 점검 시스템을 통하여 저장된 데이터들의 암호화 및 복호화 가능 여부를 탐지하여 비인가 사용자들의 사용을 방지한다.

데이터 백업/관리 모듈은 사용자의 부주의로 인한 데이터 삭제, 악의적인 사용자의 삭제 및 바이러스 감염으로 인해 해당 데이터를 정상적으로 사용하지 못할 경우를 방지하기 위해 사용자들의 데이터를 백업시켜두었다가 요청할 경우 데이터를 복구시켜준다.

4.5 접근제어 시스템

접근제어 시스템은 클라우드에 접근하는 사용자 및 디바이스를 제어하는 역할을 수행한다. 또한 정당한 사용자일 경우에도 해당 사용자가 사용하는 디바이스 및 사용자의 상황 정보를 고려하여 사용자에게 적절한 권한을 부여하게 된다.

사용자/디바이스 인증 모듈은 사용자의 개인 정보(ID/PW, OTP, 생체정보, S/N 등)를 통하여 사용자 및 디바이스 인증을 수행하게 된다. 디바이스의 관리는 MDM 서버를 통하여 별도로 수행한다. 인증 정보는 클라우드 내에 DB에 저장된 데이터를 이용하여 사전에 등록된 사용자 정보 및 권한 정보 등을 획득하여 사용자의 접근 여부를 결정한다.

상황정보 모듈의 경우 각 종 디바이스를 이용하여 다양한 장소에서 서비스를 요청하는 사용자들의 접근을 제어하는 역할을 수행한다. 사용자가 이용하는 디바이스의 위치정보를 기반으로 환경, 네트워크 상태 등과 같은 상황 정보를 고려하여 접근 권한의 등급을 조절하여 부여

하게 된다. 즉, 데이터의 읽기/쓰기가 가능한 권한을 부여받은 사용자라고 할지라도 상황정보에 따라 데이터의 읽기만 가능한 권한을 부여하게 된다. 사용자의 접근요청이 발생하면 기본적으로 인증서버에 저장된 인증정보를 기반으로 사용자의 인증을 수행함과 동시에 MDM 서버를 기반으로 사용자 디바이스의 인증 및 관리를 수행하여 사용자의 적법성을 판별한다. 그 후 디바이스의 위치정보 및 네트워크 환경과 같은 사용자 컨텍스트 정보를 기반으로 사용자가 활용 가능한 데이터에 대한 접근권한을 부여한다.(단, 사용자가 설정을 통해 디바이스에 관계없이 서비스 제공을 희망하도록 설정한 경우 해당 서비스를 제공한다.)

4.6 관리 시스템

관리 시스템은 보안 이벤트 업데이트, 새로운 취약점 진단 등과 같은 전반적인 보안관제 시스템의 관리를 수행하는 시스템이다. 관제 대상 클라우드 서버의 사용자가 가장 적은 시간대를 이용하여 모의 해킹 및 취약점 진단을 실시하여, 발견된 문제점 및 취약점, 수집된 보안 관련 정보 등을 기반으로 시스템의 업데이트 및 모듈의 기능을 개선할 수 있도록 도움을 준다. 관리 시스템은 크게 보안 이벤트 수집 모듈, 취약점 진단 모듈로 구성되어 있다.

보안 이벤트 수집 모듈은 인터넷, 뉴스기사 등을 통해 수집된 각종 새로운 보안 관련 데이터를 기반으로 각 시스템 및 모듈의 성능 업데이트를 지원하며, 클라우드 서버 상에서 발생한 위협에 신속하게 대응할 수 있도록 지원한다. 취약점 진단 시스템은 사용자가 적은 새벽시간대에 수집된 보안 이벤트 및 새로운 공격기법 등을 통하여 모의 해킹을 수행하고, 새로운 보안 위협 요소들의 동향을 수집하여 새롭게 발생 가능성이 존재하거나 문제가 발생할 수 있는 부분에 대한 수정 및 보완을 진행한다.

5. 도입효과

클라우드 환경은 다양한 IT기술의 융합된 컴퓨팅 환경으로 여러 취약점이 발견될 수 있다. 또한 수많은 데이터들이 저장되어 있는 상태로 데이터의 관리 및 안전성에 대한 관심이 집중되고 있으며, 추가적으로 안정적인 클라우드 서비스의 제공이 요구되고 있다. 이러한 요구사항을 만족하기 위한 연구가 지속적으로 진행되고 있지만 아직까지 미비한 실정이다.

클라우드 환경에 보안관제 시스템을 구축할 경우 데이터 보안 시스템을 통하여 서버에 저장되어 있는 수많은 데이터의 안전한 저장 및 관리가 가능해지며, 데이터의 복사 및 이동을 탐지하여 로그를 남기고, 해당 로그를 통하여 데이터의 유출 및 침해사고를 방지할 수 있다. 또한 네트워크 보안 시스템을 통하여 바이러스, 웜 등으로 인한 서버의 문제점을 신속하게 대응하여 안정적인 서비스를 제공할 수 있다.

모니터링 시스템은 클라우드 서비스를 제공받고 있는 사용자 및 사용자의 디바이스의 행동, 데이터의 이용현황 및 내부에서 발생할 수 있는 데이터의 위·변조 등을 탐지하여 발견 즉시 대응할 수 있도록 실시간으로 모니터링을 수행한다. 기존 관제시스템의 경우 많은 인력을 투입하여 24시간 모니터링 및 관제를 수행하였으나 자동화 관제 시스템을 사용함으로써 적은 인력으로 관제 능력을 소화할 수 있을 뿐만 아니라 관제를 수행하다 놓칠 수 있는 부분을 찾아 탐지 및 진단할 수 있을 것으로 예상되며, 클라우드 환경에서 보안관제 모델에 대한 기반 연구로 활용 가능할 것으로 예상한다.

6. 결론

최근 언제 어디서나 손쉽게 서비스를 제공받을 수 있는 클라우드 환경에 대한 사용자들의 관심이 증가하고 있으며, 또한 다양한 환경에서 발생할 수 있는 다수의 위협으로부터 데이터의 안전한 관리에 대한 관심이 증가하고 있다. 이를 해결하기 위한 관련 연구가 활발하게 진행되고 있으나 다소 미비한 실정이다. 따라서 본 논문에서는 클라우드 환경에서 유무선 통합 보안관제 모델을 제안하였다. 본 논문에서 제안한 보안관제 모델은 클라우드 환경에서의 안전한 서비스를 제공하기 위한 방안으로 활용 될 수 있으며, 기타 유사한 환경에서도 활용 가능할 것으로 예상된다.

ACKNOWLEDGMENTS

This work was supported by the National Research

Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2012-010886)

This work was supported by the Soonchunhyang University Research Fund.

This work was supported by Professor Sabbatical year program (2013) of Soonchunhyang University.

REFERENCES

[1] NIST SP 800-144, “Guidelines on Security and Privacy in Public Cloud Computing”, 2011.

[2] NIST SP 800-39, "Managing Information Security Risk", 2011.03

[3] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, March, 2010.

[4] Cloud Security Alliance(CSA), “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, 2009.

[5] T. H. Kim, I. H. Kim, C. W. Min, Y. I. Um, " Trend of Cloud Computing Security Technology", KIISE 2012.

[6] H. H. Lee, "IT Planning Series " Cloud Computing Security Tresnds", 2011

[7] T. H. Kim, I. H. Kim, J. H. Kim, C. W. Min, J. H. Kim, Y. I. Um, "Security-Enhanced Local Process Execution Scheme in Cloud Computing Environments", Journal of KIISE Vol.20, No. 5, 2010

[8] V. Casola, R. Lettiero, M. Rak, and U. Villano, “Access Control in Cloud-on-Grid Systems: The PerfCloud Case Study,” Computers, Privacy and Data Protection: an Element of Choice, 427-444, 2011.

[9] D. Chen, X. Huang, and X. Ren, “Access Control of Cloud Service Based on UCON,” Lecture Notes in Computer Science, 2009.

[10] H. D. Lee, S. J. Lee, "A Study on development of evaluation indicators on the Managed Security Service(MSS)", Journal of the Korea Institute of Information Security and Cryptology, vol 22, No.5, 2012.

[11] Y. J. Kim, S. Y. Lee, H. Y. Kwon, J. I. Lim, “A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services”, Journal of the Korea Institute of Information Security and Cryptology, vol 19, pp. 103-111, 2009. 2

[12] Renaud Bidou, “Security Operation Center Concepts& Implementation”

[13] John W.Rittinghouse and James F.Randsome, “Cloud Computing Implementation, Management and Security ” in CRC Press, pp. 153-154, 2010,

[14] B. Sotomayor, R. Montero, I. Llorente, and I. Foster, “Virtual Infrastructure Management in Private and Hybrid Clouds,” IEEE Internet Computing, Vol.13, No.5, pp. 14 - 2, 2009.

[15] R.M.Savola and P.Heinonen, “Security Measurability Enhancing Mechanisms for a Distributed Adaptive Security Monitoring System,” IEEE 4th International Conference on Emerging Security Information System and Technology, pp. 25-34, 2010.

변 연 상(Byun Yun Sang)

・2012년 2월 : 순천향대학교 정보보호학과(공학사)
・2013년 3월 ~ 현재 : 순천향대학교 정보보호학과 석사과정
・관심분야 : 클라우드 컴퓨팅 보안, 스마트워크 보안, 개인정보보호, 보안관제, 암호 프로토콜 등
・E-Mail : ysbyun@sch.ac.kr

곽 진(Kwak Jin)

・2000년 8월 : 성균관대학교 생물기전공학과(공학사)
・2003년 2월 : 성균관대학교 컴퓨터공학과(공학석사)
・2006년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
・2007년 3월 ~ 현재 : 순천향대학교 정보보호학과 교수
・관심분야 : 자동차 보안, 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안
・E-Mail : jkwak@sch.ac.kr