안전한 클라우드 서비스 환경을 위한 다중 웹 방화벽

오지수*, 이승현*, 박민우*, 정태명**
*성균관대학교 전자전기 컴퓨터공학과
**성균관대학교 정보통신공학부
{jsoh, shlee87, mwpark}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

Multiple Web Application Firewalls for Secure Cloud Services

Ji-Soo Oh*, Seung-Hyun Lee*, Min-Woo Park*, Tai-Myoung Chung**
*Dept of Computer Engineering, Sungkyunkwan Univ.
** College of Information and Communication Engineering, Sungkyunkwan Univ.

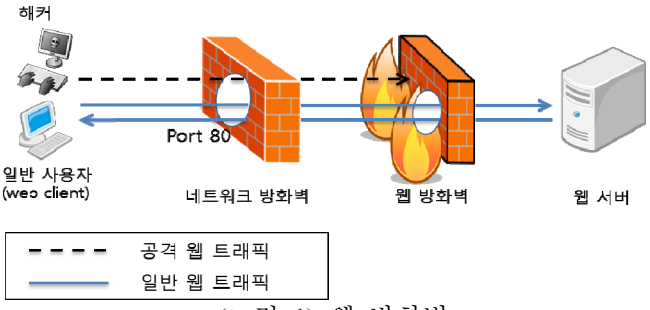
요 약

클라우드 컴퓨팅은 최근 IT 기술 중 가장 주목받는 분야로, 클라우드 컴퓨팅 자원을 네트워크 기반으로 제공하는 기술이다. 클라우드 환경에서 소프트웨어를 개발하는 경우 가상 환경을 이용해서 작업 비용을 대폭 절감할 수 있는 이점이 있지만, 웹 어플리케이션 취약점을 이용한 웹 기반 공격 등의 보안 문제가 남아있다. 클라우드 컴퓨팅이 인터넷을 통해서 서비스를 제공하기 때문에 웹 보안 향상이 클라우드 컴퓨팅의 중요한 보안 이슈이다. 본 논문에서는 클라우드 시스템의 웹 보안 문제를 해결하기 위해 클라우드 컴퓨팅을 기반으로 다중 웹 방화벽(Web Application Firewall)을 구축하는 방안을 제안하고자 한다.

1. 서론

최근 전세계적으로 주목받고 있는 IT 기술 중 하나인 클라우드 컴퓨팅은 차세대 컴퓨팅 환경으로 많은 기업의 관심을 받고 있다. 클라우드 컴퓨팅은 IT 서비스와 추상화된 자원을 네트워크 기반으로 제공하는 기술이다. 가트너는 클라우드 컴퓨팅을 “고객들에게 인터넷 기술을 활용해서 높은 수준의 확장성을 가진 자원들을 서비스로 제공하는 컴퓨팅 스타일”이라 정의한다[1]. 클라우드 시스템은 클라우드 컴퓨팅 자원을 소비자의 요구에 따라 공유해서, 소프트웨어 개발 시 초기 작업 비용이 절감되고 서비스 사업자가 시스템을 탄력적으로 운영할 수 있다.

하지만 클라우드 시스템의 보안상 문제점이 지적되면서, 클라우드 컴퓨팅의 많은 장점에도 불구하고 기업 및 단체에서 클라우드 서비스를 사용하는 데 어려움을 겪고 있다. 클라우드 컴퓨팅의 보안 문제점은 [1], [2], [3] 외에 다수의 자료에서 지적하고 있다. 대표적인 보안 문제로 웹 어플리케이션 취약점이 있다[1]. 클라우드의 가상머신이 웹에 연결되어 각각을 웹 서버로 활용할 수 있기 때문에, 웹 어플리케이션의 취약점을 이용한 웹 기반 공격이 클라우드 시스템의 중요한 보안 문제이다. 웹 기반 공격으로는 인젝션 공격과 크로스 사이트 스크립트 등이 있으며, 이러한 공격은 클라우드 서비스를 이용하는 사용자에게는 기밀정보 유출 등의 피해를 입히고, 클라우드 사업자는 가상화 취약점을 이용하는 악성코드에 감염될 수 있다. 따라서 웹 보안 향상은 클라우드 컴퓨팅 보안 문제에서 주목해야 할 이슈이다.



(그림 1) 웹 방화벽

웹 방화벽(Web Application Firewall)은 웹 서버를 해커의 공격으로부터 지켜내기 위한 정보보안 기술이다. 사용자와 웹 서버의 사이에 위치하여 사용자의 요청을 규칙에 따라 필터링해서 전달하는 역할을 한다. 웹 방화벽은 기존의 네트워크 방화벽과 달리 암호화된 공격 트래픽도 필터링 할 수 있다는 장점을 가지며 (그림 1)이 설명하고 있다.

본 논문에서는 클라우드 컴퓨팅 시스템을 공격하는 악성 트래픽 탐지를 개선하는 다중 웹 방화벽 구축 방안을 제안한다. 웹 방화벽을 통해 각 가상머신의 웹 기반 서비스에 대한 공격을 막아 웹 보안을 향상시키는 것에 목적을 둔다.

본 논문의 구성은 다음과 같다. 2 장 관련연구에서는 클라우드 컴퓨팅의 보안 이슈, 웹 어플리케이션 보안, 웹 방화벽 그리고 클라우드 기반 방화벽에 대해 설명하고 3 장에서는 클라우드 서비스 환경의 보안 향상을 위한 다중 웹 방화벽 형태를 제안하며 4 장에서 결론을 맺는다.

2. 관련연구

2.1 클라우드 컴퓨팅 보안 이슈

클라우드 컴퓨팅은 배포 형태를 IaaS 와 PaaS, SaaS 세 가지로 분류할 수 있으며, 서비스 모델에 따라 요구하는 보안 수준이 다르다. IaaS 는 가상 서버, 가상 스토리지와 같은 서버 인프라를 제공하는 서비스이다. IaaS 의 가장 큰 보안 위협요소는 가상화 엔진인 하이퍼바이저의 취약점을 이용한 공격이다. PaaS 는 소프트웨어 개발을 위한 플랫폼을 제공하는 서비스이다. 해커가 플랫폼을 분석해서 클라우드 인프라를 제어하게 되는 경우를 방지하는 것이 PaaS 의 주요 보안 이슈이다. SaaS 는 클라우드 컴퓨팅 사업자가 소프트웨어를 제공하고, 사용자가 인터넷을 통해서 해당 서비스를 제공받는 모델이다. 따라서 SaaS 의 보안 이슈는 웹 어플리케이션에서 발생하는 다양한 보안이슈와 유사하다[1].

2.2 웹 어플리케이션 보안

웹 어플리케이션 보안은 웹 어플리케이션에 존재하는 보안 취약점을 악용한 공격으로부터 웹 서버를 보호하는 것을 의미한다. 대표적인 웹 기반 공격은 국제 웹 보안 표준기구(OWASP)가 2010 년에 발표한 10 대 취약점을 예로 들 수 있으며, (표 1)이 분류하고 있다[9]. 해커는 이러한 취약점을 통해 웹 사이트와 웹 어플리케이션을 공격하여 기밀 정보를 유출하거나 정보를 변조한다. 웹 어플리케이션 보안은 인터넷을 통해 제공되는 클라우드 서비스에서도 동일하게 적용된다. 클라우드 서비스 사업자와 사용자 모두가 웹 기반 공격에 노출되어 있으며 개인정보 유출로 심각한 피해를 입을 수 있다. 하지만 기존의 방화벽과 침입차단 시스템은 암호화 된 웹 트래픽은 검사할 수 없기 때문에 웹 어플리케이션 보안에 적합하지 않다. 웹에 기반한 공격으로부터 클라우드 시스템을 보호하기 위해서는 이러한 공격에 대응하기 위한 목적으로 개발된 정보보호 기술을 클라우드 시스템에 적용시켜야 한다.

<표 1> OWASP 10 대 취약점

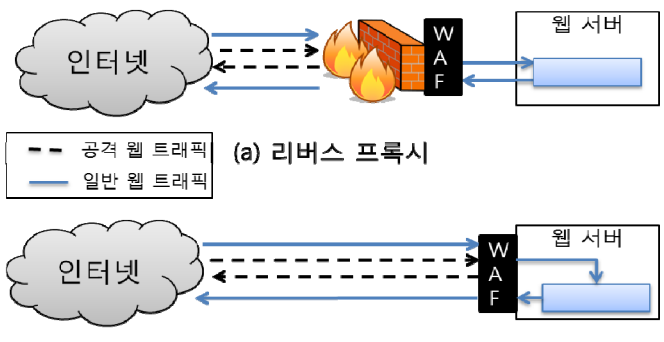
1	Injection
2	Cross Site Scripting
3	Broken Authentication and Session Management
4	Insecure Direct Object Reference
5	Cross Site Request Forgery
6	Security Misconfiguration
7	Insecure Cryptographic Storage
8	Failure to Restrict URL Access
9	Insufficient Transport Layer Protection
10	Unvalidated Redirects and Forwards

2.3 웹 방화벽(Web Application Firewall)

웹 방화벽은 웹 기반 공격으로부터 웹 서버를 보호하기 위한 정보보안 기술로 웹 서버와 클라이언트의 사이에 위치하여 7 계층 메시지를 분석한다. 웹 방화벽은 HTTP / HTTPS / SOAP / XML-RPC / 웹 서비스 계층의 모든 요청과 응답을 검사한다. 웹을 통해 들어오는 클라이언트의 요청을 미리 정의된 규칙으로 필터링하여 정상적인 요청만을 웹 서버로 전달한다. 그리고 요청에 대한 응답도 웹 방화벽을 거쳐 필터링된 후 클라이언트에게 전달된다. 웹 방화벽은 웹 사이트와 웹 어플리케이션을 공격으로부터 보호 할뿐만 아니라, 웹 사이트의 위· 변조를 방지하여 피싱을 예방할 수 있다.

웹 방화벽은 일반적으로 5 개의 과정을 거쳐 웹 트래픽을 검사한다[7]. 첫 번째로 웹 서버로 들어오는 요청을 파싱한다. 두 번째로 파싱된 요청을 표준 형태로 변환시키는 normalization 과정을 수행한다. 웹 시스템은 다른 연관 시스템과 조합하여 설계되는 경우가 많기 때문에, 공격 트래픽을 일반 트래픽으로 보이게끔 형태를 바꾸는 것이 가능하다. 이러한 경우를 예방하기 위해 표준 형태로 바꾸어 준다. 세 번째로 시스템에 설정된 기본적인 보안 체크를 수행한다. URL encoding validation 이나 unicode encoding validation 을 예로 들 수 있다. 네 번째로 정규표현식으로 구성된 규칙으로 입력 문장을 비교하는 과정이 있으며, 마지막으로 결과를 기록한다.

웹 방화벽의 운영 방식은 두 가지 종류로 나누어 살펴볼 수 있다. 웹 방화벽의 가장 일반적인 운영 방식은 리버스 프록시 방식으로, (그림 2)의 (a)를 통해 확인할 수 있다. 리버스 프록시 방식은 웹 방화벽이 웹 서버와 외부 네트워크 사이에 설치되어 프록시 역할을 하게 된다. 클라이언트에서 웹 서버로의 접근이 한 곳으로 모여서 시스템 관리자가 공격을 추적하기에 용이하며, 프록시 밖의 클라이언트가 내부 서버에 대해 파악할 수 없어 보안을 향상시킬 수 있다. 또 다른 운영 방식은 웹 방화벽이 웹 서버의 플러그 인으로 설치되는 형태로, 임베디드 방식이라 부르며 (그림 2)의 (b)에서 설명하고 있다. 임베디드 방식은 리버스 프록시 방식과는 달리 웹 서버의 익명성을 보장할 수 없다는 한계를 갖는다.



(그림 2) 웹 방화벽의 네트워크 토폴로지

웹 방화벽은 웹 트래픽의 공격 여부를 판단하는 필터링 방식에 따라 negative security model 과 positive security model 로 나눌 수 있다. negative security model 은 악성 트래픽 정보를 데이터베이스화한 뒤, 클라이언트가 웹 서버에 전송한 요청이 사전에 정의된 공격과 일치하면 차단하고 그 외에는 모두 허용하는 방식이다. 이 방식의 경우 알려진 공격에 대해서는 정확하게 필터링할 수 있지만, 존재가 널리 알려지지 않아 아직 보완되지 않은 취약점을 악용하는 제로 데이 공격은 차단하기 어렵다. Negative security model 이 요청의 공격 여부를 판단한다면, positive security model 은 요청이 정상적인 요청인지를 확인하는 방식이다. Positive security model 은 정상적인 요청을 정의해서, 클라이언트의 요청이 정상 요청으로 판단되지 않는 경우 모두 차단한다. Negative security model 과는 달리, 제로 데이 공격을 포함한 거의 모든 공격을 필터링할 수 있다는 장점을 가지고 있다. 하지만, 이 필터링 방식은 정상적인 트래픽을 정의하기가 어려우며, 악성이 아닌 일반 트래픽을 필터링 할 확률이 높다는 단점이 있다.

2.4 클라우드 기반 방화벽

일반적인 방화벽은 고객이 제품을 구매한 다음, 그 고객의 보안 요구사항에 맞춰서 보안 정책을 구성하는 정적인 보호 체계를 제공한다. 일반적인 방화벽이 수동적인 방어 방식이라면, 클라우드 기반의 방화벽은 능동적인 방어 방식을 제공한다고 할 수 있다. 클라우드 기반 방화벽은 클라우드 상에 구축한 웹 서버를 이용해서 보안 위협에 대한 정보를 실시간으로 공유하는 시스템이다. 시스템의 어딘가에서 공격이 발견되면 그 정보가 클라우드 웹 서버를 통해 다른 곳으로 빠르게 전달되어 전체 시스템이 위협 요소에 대응할 수 있게 된다. 클라우드의 전체 시스템이 서로 협력하여 정보를 공유해서, 공격에 대한 정보가 실시간으로 업데이트 될 수 있고 더 빠르게 공격에 대한 대응책을 찾아낼 수 있다[8]. 클라우드 기반 방화벽은 가상 자원을 이용해서 서버 구축이 간단해 지고 비용이 절감된다는 장점도 갖는다.

3. 클라우드 기반 다중 웹 방화벽

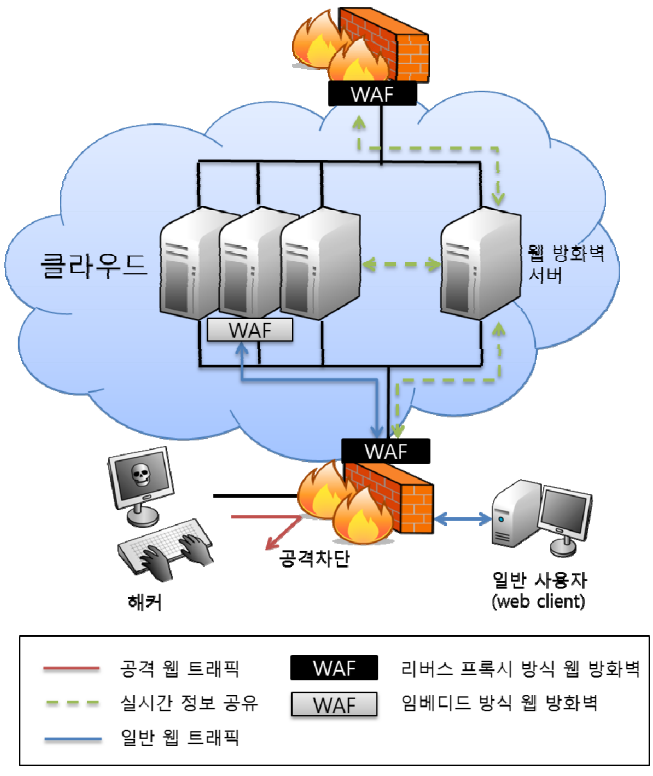
3.1 클라우드 시스템의 웹 보안 필요성

Platform as a Service(PaaS)는 클라우드 컴퓨팅의 서비스 모델 중 하나로, 소프트웨어 개발을 위한 플랫폼을 제공한다. PaaS 를 사용하는 서비스 개발자들은 PaaS 사업자가 제공한 플랫폼 상에서 IT 자원을 활용하여 새로운 웹 어플리케이션을 개발한다[2]. PaaS 사용자의 웹 어플리케이션이 인터넷을 통해 클라이언트에게 제공되는 경우, 해커가 웹 어플리케이션 취약점을 이용해서 웹 서버를 공격할 수 있다. 이러한 웹 기반 공격은 기밀문서를 유출하거나 정보를 변조시켜서 PaaS 사용자와 어플리케이션의 클라이언트 모두에게 큰 피해를 일으킬 수 있다. 또한 가상화 취약점을 이용하는 악성코드가 웹을 통해 유입되는 경우, 해커가 게스트 OS 파일 시스템에 대한 제어 권한을 획득하거나 프로세스를 모니터링 할 수 있게 되어 클라우드 시스템 전체에 심각한 보안 위협이 된다. 웹 방화벽은 이런 웹 기반의 공격들을 방어하여 웹 보안을 향상시키는 솔루션 중 하나로, 클라이언트의 요청을 필터링해서 공격 트래픽이 웹 서버에 도달하지 못하도록 한다.

PaaS 사용자는 웹 어플리케이션 취약점을 이용한 공격에 대응하기 위하여 웹 서버에 임베디드 방식의 웹 방화벽을 설치할 수 있다. 하지만 임베디드 방식의 웹 방화벽은 리버스 프록시 방식과 달리 웹 서버에 익명성을 제공하거나 외부 네트워크와 클라우드 시스템을 분리하는 등의 보안 기능을 제공할 수 없기 때문에 보안 향상에 한계를 갖는다. 리버스 프록시 방식의 웹 방화벽은 클라우드 시스템과 외부 시스템의 경계에 설치되어 PaaS 사용자는 설치할 수 없다. 따라서 PaaS 사업자가 리버스 프록시 방식의 웹 방화벽을 설치해야 하며, 이를 통해 전체 클라우드 시스템의 웹 보안을 향상시킬 수 있다.

3.2 클라우드 기반 다중 웹 방화벽 구성

본 절에서는 클라우드 기반 다중 웹 방화벽의 구조에 대해 설명한다. 클라우드 기반 다중 웹 방화벽은 클라우드 시스템의 경계에 설치되는 리버스 프록시 형태의 웹 방화벽과 사용자에 의해 개별 가상 머신에 설치되는 임베디드 웹 방화벽으로 구분된다. 두 방식은 아래 (그림 3)과 같은 형태로 구성되며, 이는 사용자 수준에서 요구되는 웹 어플리케이션 보안과 클라우드 컴퓨팅 사업자 수준에서 요구되는 클라우드 컴퓨팅 보안을 만족하기 위한 구조이다.



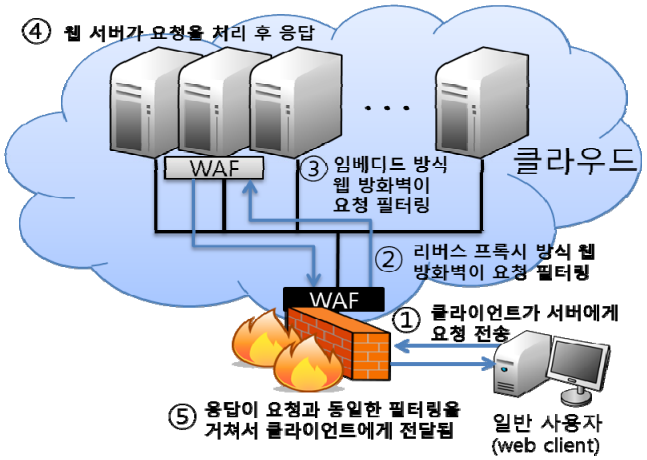
(그림 3) 클라우드 기반 다중 웹 방화벽

클라우드 기반 다중 웹 방화벽은 리버스 프록시 방식과 임베디드 방식을 혼용한다. 리버스 프록시 방식은 클라우드 시스템으로 유입되는 모든 트래픽에 대해 검사 규칙을 적용한다. 리버스 프록시 방식의 웹 방화벽은 시스템 사용자 전체의 보안을 위해 설치되며, 사전에 정의된 정책에 따라 모든 유입 트래픽을 검사한다. 임베디드 방식은 개별 사용자에 의해 선택적으로 설치된다. 리버스 프록시 방식이 전체 시스템에 포괄적인 보안 정책을 적용했다면, 임베디드 방식은 개별 사용자가 직접 설계한 정책을 적용시킨다.

그 결과 리버스 프록시 방화벽과 임베디드 웹 방화벽은 각각 다른 탐지 방식을 이용한다. 먼저 리버스 프록시 방식의 웹 방화벽은 negative security model 로 웹 트래픽을 필터링한다. 리버스 프록시 방식은 전체 클라우드 시스템에 대한 포괄적인 보안을 적용하기 때문에, 잘 알려진 공격 트래픽을 탐지하고 이를 차단하기에 유용한 negative security model 을 사용한다. 이와 달리 임베디드 방식 웹 방화벽은 positive security model 로 웹 트래픽을 필터링한다. 클라우드 시스템의 경계에서 1 차적인 알려진 공격 트래픽에 대한 탐지가 제공되기 때문에 내부에 존재하는 임베디드 방식의 웹 방화벽은 positive security model 을 통해 알려지지 않은 공격을 탐지하고 이를 자신의 서비스에 맞게 대응하는 정책이 필요하다.

3.3 클라우드 기반 다중 웹방화벽 동작 과정

(그림 4)는 클라우드 기반 다중 웹 방화벽의 필터링 과정을 설명한 그림이다. 클라이언트가 웹 서버에 요청을 전송하면 그 요청은 먼저 리버스 프록시 방식의 웹 방화벽에서 negative security model 로 필터링된다. 클라이언트의 요청을 알려진 공격과 비교해서 악성트래픽을 탐지하고 정상적인 요청만을 웹 서버에 전달한다. 웹 서버가 임베디드 웹 방화벽을 사용하고 있다면 positive security model 로 한번 더 필터링한다. 정의된 정상 요청이 아니면 삭제하고, 정상 요청만을 전달한다. 웹 서버는 요청을 처리해서 사용자에게 응답을 전송한다. 웹 서버의 응답도 두 번의 필터링을 거친 후 요청을 보냈던 클라이언트에게 전달된다.



(그림 4) 웹 트래픽 필터링 과정

4. 결론

클라우드 컴퓨팅은 가상 환경에서 컴퓨팅 자원을 공유해서 시간과 비용 모두를 절감할 수 있는 기술로, 최근 IT 분야에서 가장 주목받고 있다. 클라우드 서비스에 대한 수요가 급증함에 따라 클라우드 컴퓨팅 보안이 중요한 이슈가 되었다. 지금까지 본 논문에서는 클라우드를 기반으로 리버스 프록시 방식과 임베디드 방식 두 가지 형태의 웹 방화벽을 구축해서 클라우드 시스템의 모든 웹 서버의 웹 보안을 향상시키는 방안에 대해 제안하였다. 클라우드를 기반하여 실시간으로 보안 위협 정보를 공유해서 공격에 대해 동적으로 대응하고, 웹 방화벽의 두 가지 필터링 방식을 모두 사용해서 보안 강도를 높였다. 향후 연구 방향으로 두 번의 필터링을 거쳐도 퍼포먼스가 크게 저하되지 않기 위한 연구가 필요하며, 클라우드 환경의 이점을 더욱 활용하기 위해 웹 방화벽과 가상화 기술을 접목한 발전된 형태를 개발하기 위해 연구해야 할 것이다.

ACKNOWLEDGMENT

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음. [10041244, 스마트 TV 2.0 소프트웨어 플랫폼]

참고문헌

[1] Subashini, S. and Kavitha, V, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications Volume 34 Issue 1 1-11, Jan 2011

[2] 김학범, “클라우드 컴퓨팅 환경에서의 보안관리에 대한 연구”, 경영컨설팅리뷰 제 2 권 제 1 호 127-144,Feb 2011

[3] Minqi Zhou , “Security and Privacy in Cloud Computing: A Survey”, Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on 105-112, Nov 2010

[4] 김수용, “사용자 관점의 보안정책 자동 학습 능력을 가진 Web Application Firewall”, 한국인터넷정보학회 2003 년도 추계학술발표대회 논문집 295-298, Nov 2003

[5] Ivan Ristic et al., “Web Application Firewall Evaluation Criteria”, Web Application Security Consortium, 2006

[6] R Mohd Ikram, “Web Application Firewall”, Faculty of Information Technology and Quantitative Science Universiti Teknologi Mara, May 2006

[7] Namit Gupta, “Web Application Firewall”, CS499 : B.Tech Project Final Report

[8] Weili Huang, “New Network Security Based on Cloud Computing”, Education Technology and Computer Science (ETCS), 2010 Second International Workshop on 604-609, Mar 2010

[9] J. Williams, D. Wichers, “OWASP top 10 – 2010”, OWASP Foundation, Apr 2010