디지털산업정보학회 논문지 제14권 제2호-2018년 6월
http://dx.doi.org/10.17662/ksdim.2018.14.2.011

블록체인을 적용한 사설 클라우드 기반 침입시도탐지

이 세 열*

A Probe Detection based on Private Cloud using BlockChain

Lee Seyul

〈Abstract〉

IDS/IPS and networked computer systems are playing an increasingly important role in our society. They have been the targets of a malicious attacks that actually turn into intrusions. That is why computer security has become an important concern for network administrators. Recently, various Detection/Prevention System schemes have been proposed based on various technologies. However, the techniques, which have been applied in many systems is useful for existing intrusion patterns on standard-only systems. Therefore, probe detection of private clouds using BlockChain has become a major security protection technology to detection potential attacks. In addition, BlockChain and Probe detection need to take into account the relationship between the various factors. We should develop a new probe detection technology that uses BlockChain to fine new pattern detection probes in cloud service security in the end. In this paper, we propose a probe detection using Fuzzy Cognitive Map(FCM) and Self Adaptive Module(SAM) based on service security using BlockChain technology.

Key Words : BlockChain, Fuzzy Cognitive Maps, Private Cloud, Probe Detection

Ⅰ. 서론

4차산업사회는 사물인터넷, 클라우드, 빅데이터, 모바일의 기술은 4차산업의 중요한 기본요소에 해당되며 각각의 기술에 대한 보안이슈는 매우 중요하게 여겨지고 있다. 특히 오늘날과 같이 사이버 공격 패턴의 다양화로 인해 침입탐지 및 침입방지에 대한 이슈는 매일 언론매체에 자주 등장하는 소식 중에 하나로 여겨지고 있다. 이에 많은 보안업체들은 가성비가 뛰어나고 강력한 보안이 제공되고 있는 침입탐지 및 방지기술에 매진을 하고 있는 추세이다. 그러나 보안업체의 제품들은 각각의 제품이 우수한 성능을 제공하고 있으며 다른 경쟁업체 제품에 비하여 어떠한 특징과 장점이 있다고 또는 자사의 제품의 우수성을 입증하고자 보안시장에서의 어떠한 영역부분에서 1위를 하고 있다고 선전을 하고 있을 것이다. 그러나 관점을 조금만 다르게 보면 경쟁업체의 제품들을 서로 인정하면서 위협정보, 침해정보 등에 대한 상호정보공유를 하면 부족한 기능부분에 대하

* 청운대학교 컴퓨터공학과 교수

여서는 보완될 것이며 우수성이 입증된 기능에 대하여서는 상승하는 효과가 있을 것이다. 물론, 경쟁제품간의 탐지 및 방지엔진의 종류에 따라 정보를 저장하는 방식, 탐지하는 기법 등이 서로 다른 경우도 있을 것이다. 이에 각 제품 간에 침해정보를 중앙집중 클라우드에 업로드 하여 실시간 위협정보 또는 과거의 침해정보 등에 대한 내용문서를 스토리지에 저장하고 각 제품 간에 필요한 정보를 실시간으로 다운로드 하는 클라우드 공유체계를 구축하면 KISA에서 기존에 구축되어 있는 C-TAS 침해정보공유체계보다 더 우수한 성능을 발휘할 것이다.

위협정보 중앙 집중화는 각 업체의 제품에서 처리되는 정보에 대하여 보관, 전달, 관리에 이용하는 기술로 위협정보 관리시스템을 통한 위협정보 관리 기능과 중앙 저장소를 이용하여 각 제품이 습득하지 못한 정보를 탐지 및 방지 엔진에 업데이트 할 수 있다. 하지만 모든 정보가 중앙 스토리지에 저장되어 있으므로, 직접 중앙 스토리지를 노린 공격이 발생하여 위협정보가 오히려 유출될 경우가 발생하면 해커들에게는 각 제품에 대한 침입탐지 및 방지 룰(rule)에 대한 대응을 할 수 있어 큰 문제점으로 발생할 수도 있다. 이에 클라우드의 뛰어난 가성비를 활용하고 중앙 집중된 위협정보에 대한 탈취를 원천 차단 할 수 있는 기능제공이 요구된다.

기존 탐지기법 중 네트워크 기반의 탐지기법은 정적인 특징을 가지는 룰(rule)을 기본적으로 사용하기에 사물인터넷 및 클라우드 이슈 이전의 환경에서는 크게 문제가 되지 않았으나 최근 동적인 환경을 가지는 사물인터넷 및 클라우드 같은 새로운 이슈의 등장으로 동적인 환경에 맞는 탐지기법을 고려할 수밖에 없는 실정에 이르렀다. 정적인 특징을 가지는 네트워크기반 탐지기법은 동적인 환경 변화를 고려하기에는 한계가 있으며, 이러한 한계는 탐지성능 저하로 이어 질 것이다.

그러므로 오늘날은 네트워크 기반 탐지에 동적인 환경을 고려 할 수 있는 방법이 필요하게 되었고 이에 본 논문에서는 저자가 개발한 적응형 퍼지인식도가 적용된 침입시도탐지기법에 추가로 동적인 환경을 고려할 수 있는 자가 적응 모듈(Self Adaptive Module)을 사용하여 동적인 환경 변화를 고려하기 위한 적응형 룰(rule)을 생성하고 이를 퍼지인식도가 적용된 침입시도탐지에 추가하는 하이브리드 침입시도탐지모델을 제안하고 안전한 클라우드 기반의 중앙 집중형 위협정보를 탈취할 수 없는 블록체인 기술을 접목한다.

본 논문의 구성은 다음과 같다. 2장에서는 클라우드 서비스를 위한 보안 요구 사항을 살펴보고, 3장에서는 블록체인기술이 적용된 클라우드 기반 침입시도 탐지를 다루며 마지막으로 4장에서는 결론과 향후 연구 과제를 논한다.

Ⅱ. 관련연구

2.1 퍼지인식도가 적용된 침입시도탐지(FCM)와 자가 적응 모듈(SAM)

퍼지인식도가 적용된 침입시도탐지의 탐지모듈 중 판단모듈에 퍼지인식도(Fuzzy Cognitive Maps : FCM)의 Causal Knowledge Reason(CKR)을 이용하여 지능적 판단모듈을 구성한다[1, 2]. 아울러, 자가 적응 모듈에 사용하는 것은 IBM에서 제안한 MAPE-K를 이용하며 저자의 2017년 논문에 제시한 바 있다[3].

2.2 사설 클라우드에서 고려할 보안 사항

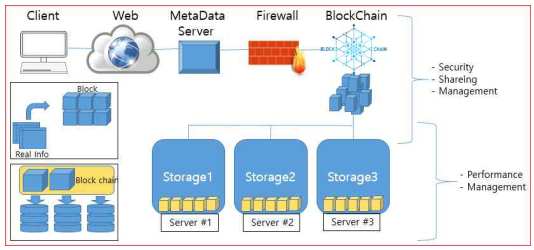
블록체인의 가장 많이 활용되는 플랫폼은 이더리

움 플랫폼 이지만 스토리지 저장 및 블록체인 합의 과정에 대해 적응하기 어려움이 있다. 전체적인 네트워크에 대해 단일 상태가 필요하지 않으므로 폭넓은 합의를 하도록 알고리즘 및 플랫폼을 구성해야 한다. 또한, 공중망에서 클라우드 시스템에서는 블록체인이 클라이언트에게 블록이 나눠지는 구조이다. 클라이언트 탐색기를 Namespace Extension 기반으로 구성하면 기존 윈도우 탐색기에서 사용하는 단축키, Drag & Drop, 파일 복사, 이동, 삭제, 온라인 파일 첨부, 외주 저장 등 기존 사용자 환경에 맞게 커스텀을 하면서 기밀성을 유지해야 한다. 하지만 일부 온라인 첨부시 브라우저마다 별도의 커스텀 탐색기를 사용하는 경우에 Namespace Extension으로 만든 객체가 지원이 안 되는 경우가 있기 때문에 별도의 플러그인을 구성하여 사용자에게 가용성을 제공해야 한다. 정보 업/다운로드 시 보안으로는 각 제품별 업체의 사용자에 의해 수정이 필요하거나 읽기가 필요한 경우 클라우드에 있는 위협정보를 요청받아 보게 되는데, 이때 갈무리제어, 클립보드에 대한 제어, 출력에 대한 제어를 하여 카피본이 생성되지 않도록 보호해야 한다. 인터넷이 차단되어 네트워크가 불가능한 상태가 발생하는 경우가 고려되어야 한다. 클라우드 기반이기에 온라인에서만 위협정보의 업/다운로드가 가능하지만 서버가 다운이 되었을 경우에 대비하여 오프라인 모드를 구성할 수 있어야 한다.

Ⅲ. 클라우드 보안 기반 침입시도탐지

3.1 블록체인기반 클라우드 서비스 보안

본 연구에서는 정보를 외부 및 내부의 악의적 행위로부터 안전하게 보호하고 활용성을 극대화하는 것이다. <그림 1>과 같이 클라이언트 단말이 유, 무선 통신망을 통하여 클라우드 서버와 연결되는 클라우드 컴퓨팅 환경에서 클라우드 서버의 정보를 보안하기 위한 것으로 클라우드 서버는 클라이언트 단말의 요청에 응답해서 클라우드 컴퓨팅 서비스를 제공하며 외부 및 내부 통신망을 통해 접속 가능하며, 파일과 폴더에 대한 목록 리스트로 이루어진 환경정보 파일을 제공하는 메타데이터 서버 및 내부 통신망을 통해 접속 가능하며 서버에서 제공되는 파일에 대한 실질적인 데이터를 저장하는 스토리지 서버로 이루어진 것을 특징으로 하는 클라우드 컴퓨팅 환경에서 클라우드 서버의 정보를 보호하여 서비스를 제공하는 것이다.



<그림 1> 블록체인기반 클라우드 서비스 보안 구조

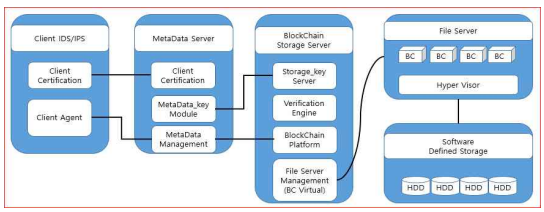
클라우드 서버를 물리적으로 분리된 메타데이터 서버와 스토리지 서버로 각각 분리하고 메타데이터 서버는 내부 및 외부 통신망을 통해 접근 가능하게 하고 스토리지는 내부 통신망을 통해서만 접근 가능하게 하며, 이와 같은 방식으로 클라우드 서버에 구비된 메타데이터 서버에는 환경정보파일 외에는 파일을 가지고 있지 않고 전달하는 역할만 하게 됨으로써 클라우드의 위협정보를 이용하는 IDS/IPS에게는 메타데이터 서버만 접근이 가능하게 하여 악의적인 해커로부터 보호를 할 수 있으며 만약 메타데이터 서버가 해킹을 당한다고 하여도 해당 서버에는 실질적인 정보가 없기 때문에 정보의 유출을 막을

수 있다.

<그림 1>을 살펴보면, 스토리지 서버에서 메타데이터 서버를 거쳐 IDS/IPS에게 정보가 전달되기 위해서는 인증과 메타데이터 서버의 인증을 통해서만 정보를 다운로드 할 수 있으며 이에 대한 인증 방법은 블록체인 기반 기술을 활용한다. 스토리지 서버는 은행과 같이 개인용 금고를 생성하여 은행에서처럼 돈을 보관하는 것과 같이 IDS/IPS의 파일을 여러 개의 서버에 분산하여 저장하고 있으며 이때 IDS/IPS가 파일을 요청하는 경우 메타데이터 서버에서 IDS/IPS에 대한 인증을 거친다. 이때 IDS/IPS는 최초 메타데이터 서버에서 발근된 인증키를 기반으로 메타데이터 서버에 인증을 받는다. 인증이 통과된 경우에는 메타데이터 서버를 통해서만 스토리지 서버에 접근이 가능하며 이때 메타데이터 또한 스토리지 서버에 인증을 받아야만 파일에 접근할 수 있다. 클라이언트 IDS/IPS가 위협정보를 저장하게 되면 파일이 MetaData Server에 저장된 것처럼 보이지만 실제로는 방화벽을 거쳐 Server #1~3에 분산 저장된다. 이 과정을 살펴보면 블록체인 스토리지 기술이 적용된 Server#1~3에는 BC(Block Chain 영역)과 Storage 영역이 논리적으로 분리되어 있으며 실제 정보(Real Info)는 보안을 위해 각각의 BC1~6에 분산되어 저장된다. 그리고 3개의 스토리지는 BC Data를 일부 중복적으로 보유하고 있어, 이중 한 대에 장애가 발생하더라도 손실된 자원을 자동으로 복구할 수 있다.

3.2 블록체인 보안 기술

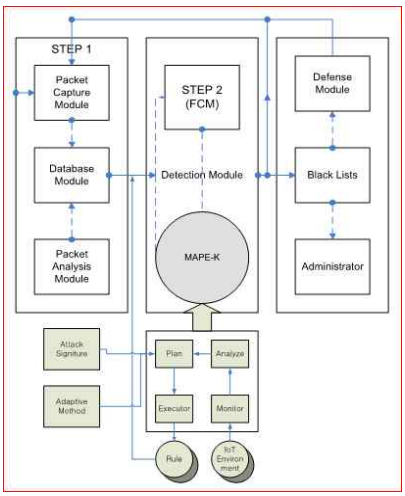
<그림 2>와 같이 블록체인 보안 기술의 Client, MetaData Server, BlockChain Storage Server, Info Server, Software Defined Storage 등의 단위 모듈별 기능에 대하여 알아본다. 첫 번째로 Client는 실제 정보를 업/다운로드 하는 IDS/IPS로 MetaData Server로부터 폴더, 파일, 속성에 대한 정보를 가져와서 탐색기 형태로 보여주는 역할을 한다. MetaData Server는 클라이언트 IDS/IPS별로 폴더, 파일, 속성에 대한 정보를 가지고 있는 서버이며 BlockChain Storage Server와 합의 및 인증을 통해 위협정보를 불러오는 중계 역할을 하는 서버이다. BlockChain Storage Server는 클라이언트가 위협정보를 업로드시 파일을 블록단위로 분산 저장하는 기능과 분산 저장된 파일을 검증하여 보여주는 역할을 하는 서버이다. File Server는 실제 블록화된 블록과 저장소간의 관리하기 위한 매니지먼트 모듈이며 Software Defined Storage는 실제 블록이 분산되어 저장되는 저장소이며 1-N개의 블록들이 중복 저장된다.



<그림 2> 블록체인 보안 구조

연구에서는 Private Clouds 뿐만 아니라 Public Clouds 서비스 환경에서도 적용가능하며 블록체인 기술을 융합하여 가상머신 이미지를 스토리지에 분산으로 저장하는 기법을 사용한다. 이때 검증을 위한 하이브리드 침입시도탐지모델은 저자가 <그림 3>와 같이 직접 연구하여 논문으로 발표한 모델이며 자가 적응 모듈이 적용된 FCM 기반의 하이브리드 침입시도탐지모델(FCM-Self)이다. 제안한 방법의 완벽한 검증을 위하여 public clouds환경에서 전통적인 네트워크 기반 탐지시스템인 K-Means, Fuzzy-ART, SVM 등과 탐지율을 비교 측정하고 공

신력 있는 데이터를 사용하여야 한다. 그러나 본 연구에서는 제안한 침입시도탐지모델은 private clouds 서비스 보안 적용을 위한 환경구성의 테스트베드환경에서 실험을 한다.



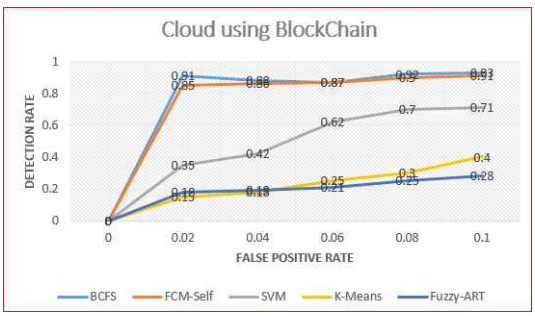
<그림 3> 자가 적응 모듈이 적용된 침입시도탐지[3]

사설 클라우드 테스트베드 환경에서의 모의 침투 테스트 해킹 툴은 Hping3와 Ostinato 0.8를 사용하고 실험에 사용된 하드웨어 환경은 Windows 10 64bit, Snort2.9.9, 그리고 Winpcap 4.1.2이며 외부 침입에 대한 탐지율과 침입에 대한 대응 능력을 확인하기 위하여 모의 침투 테스팅을 이용한다.

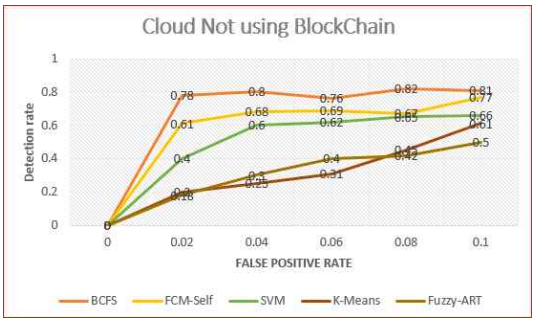
실험에서 사용한 동일한 환경은 2017년 발표한 연구와 동일한 방법과 환경에서 실시하여 블록체인이 적용한 사설클라우드 환경과 블록체인이 적용되지 않은 환경에서의 정확한 성능비교를 하도록 하여 객관성을 유지한다. Free, Normal, Busy를 정의하며 각각의 환경에서의 센서가 수집한 환경 정보의 산술평균값을 적용하여 세팅한다[4]. 아울러, 모의 침투 테스팅은 여러 형태의 침입 방법을 이용 및 실행이 가능하다. 그러나 본 연구에서는 여러 침입 방법 중 DoS 공격을 이용하여 테스트베드환경에서 수행하며 모의 침투 테스팅을 위하여 다음과 같은 세 가지 가정을 전제로 설정하고 DoS공격을 테스트 하도록 한다[5]. 본 실험에서의 모든 환경과 공격발생 환경은 저자의 2017년에 수행한 연구 환경과 완벽하게 동일하게 이루어지며 이는 객관적이 데이터 결과를 도출하여 블록체인이 적용된 사설클라우드 환경에서의 성능을 비교하기 위해서이다.

3.2 성능비교 및 결과

본 논문에서 제안한 블록체인이 사용된 클라우드 기반의 동적인 환경하의 자가 적응이 적용된 침입시도탐지(BCFS : BlockChain FCM-Self)는 <그림 4>에서 보듯이 기존의 여러 가지 탐지기법 중 K-Means, Fuzzy-ART와는 성능 차이가 발생하며 이미 여러 실험 및 평가에서 탐지능력이 객관적으로 인정된 SVM(Support Vector Machine), 그리고 2017년에 발표한 저자의 기존 FCM-Self 과도 최소 0.0에서 최대 0.6까지의 성능 개선을 보여주고 있다. False Positive error는 기존의 k-Means, Fuzzy-ART, SVM 탐지기법에 비하여 최대 2배 이상의 성능 개선을 나타내고 있음을 알 수 있으며 FCM-Self보다 전반적으로 성능개선이 되었음을 알 수 있다.



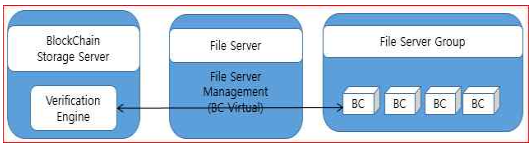
<그림 4> 블록체인이 사용된 클라우드 서비스 환경에서의 정상탐지율과 오탐지 비교



<그림 5> 블록체인이 사용되지 않은 클라우드 서비스 환경에서의 정상탐지율과 오탐지 비교

블록체인이 적용되지 않은 클라우드 서비스 환경에서의 결과는 <그림 5>와 같이 블록체인이 사용된 클라우드 서비스 환경보다는 성능의 범위가 많지는 않지만 성능 향상이 있었음을 알 수 있다.

클라우드 보안성 확보를 위한 방법으로는 블록체인을 이용한 클라우드 위협정보 탈취를 위한 인증가로채기를 하였으며 이를 위하여 MITM을 이용한 해킹공격을 사용하였고 <그림 6>과 같이 데이터 터널링 기술을 통하여 검증하였다. 이는 데이터 교류가 가장 많고 가장 많이 발생하는 검증서버(BlockChain Verification Engine)와 파일블록 임시공간(BC)간에 원활한 네트워크를 보장하는 터널기술과 클라이언트 IDS/IPS와의 인증 시스템으로 인가된 클라이언트임을 확인하고 정상적인 MetaData Server의 접속이 맞는지 BlockChain Key Server가 재확인하여 사용자의 위협정보 접근을 승인하는 시스템이며 인증된 Key 및 정보를 토대로 메타데이터 파일을 생성하고 Real Info을 BlockChain Verification Engine을 거쳐 각각의 BC에 분산저장한 뒤 결과 값을 클라이언트에게 전달하는 방식을 이용한다.



<그림 6> 데이터 터널링 구조

Ⅳ. 결론 및 연구과제

본 논문에서 기존의 다양한 침입 탐지 시스템이 클라우드와 같은 동적인 환경 변화를 고려하지 못하는 한계를 해결하고 이를 통한 탐지 성능 개선을 위한 테스트를 한 것이다. 제안한 방법에서는 동적인 환경 변화에 적용하기 위한 방법으로 자가 적응 모듈을 적용하고 블록체인기술을 도입한 클라우드 서비스 환경에서의 침입시도탐지를 제안하였다. 이를 위하여 자가 적용을 위하여 MAPE-K를 통하여 구현하며 자가 적응 모듈을 통하여 생성된 룰(rule)은 기존 침입탐지 룰(rule)에 적용함으로써 클라우드와 같은 동적 환경을 고려한 동적 적응형 침입시도탐지 모델이 기존의 침입탐지시스템 보다 탐지 성능이 개선되었음을 확인 할 수 있었으며 블록체인 기술을 적용하여 인증가로채기가 불가능함도 제시하였다.

그러나 제안한 방법에서는 테스트베드환경에서의 사설 클라우드 환경에서의 실험값이며 자가 적응을 위한 전제조건도 제시되어 있었다. 또한, 사용한 룰(rule)을 생성하기 위한 모델도 정의하였다. 이러한 전제 조건의 한계를 해결하기 위하여 향후연구에서는 공중망 클라우드환경에서의 테스트베드와 블록체인의 객관적 보안성을 확보하기 위한 다양한 검증방안에 대하여 연구가 필요하다.

참고문헌

[1] S. Y. Lee, Y. S. Kim, and B. H. Lee, “A Probe Detection Model using the Analysis of the Fuzzy Cognitive Maps,” International Conference Cyber and Security, Vol. 3480, 2005, pp. 320-328.

[2] M. Jazzar, and A. Jantan, “Towards real-time intrusion detection using fuzzy cognitive maps modeling and simulation,” International Symposium on Information Technology, Vol. 2, 2008, pp. 1-6.

[3] 이세열, “자가적응모듈과 퍼지인식도가 적용된 하이브리드 침입시도탐지모델,” 디지털산업정보학회논문지, 제13권, 제3호, 2017, pp. 19-25.

[4] J. Moon, and Y. Chang, “A Malware Detection Application Framework Based on Normal Behavior,” The Journal of the Convergence on Culture, Vol. 2, No. 1, Feb 2016, pp. 79-85.

[5] 양환석, “프로토콜 기반 분산 침입탐지시스템 설계 및 구현,” 디지털산업정보학회논문지, 제8권, 제1호, 2012, pp. 81-87.

■ 저자소개 ■

이 세 열
(Lee Seyul)

2004년 3월~현재
청운대학교 컴퓨터공학과 교수
2003년 8월 대전대학교 대학원 컴퓨터공학과 (공학박사)
2000년 1월 ~2001년 2월
(주)인소쾍 부설연구소장
1998년 7월 ~1999년 12월
한국전자통신연구원
관심분야 : 정보보안, 사물인터넷 보안, 네트워크보안, 클라우드보안, 보안관제시스템, 블록체인
E-mail : pirate@chungwoon.ac.kr

논문접수일: 2018년 06월 01일
수 정 일: 2018년 06월 08일
게재확정일: 2018년 06월 11일