Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

An Encrypted Response Model using Application Access Failure information for the Attack of IP Spoofing in a Cloud Computing Environment

Yang Liu, Sang-Bok Kim, Jae-Heung Park, Jong-Min Bae*

Department of Computer Science, Gyeongsang National University

ABSTRACT

The big data is typically collect a large amount of information. It is processed of receiving a service and is based on a cloud computing environment. These environments are easily exposed to illegal accesses, which use IP Spoofing compared to that of a single system. In this study traceback information is used to identify normal users in order to response to illegal accesses in a cloud computing environment. Then, services are provided after the identification process for the normal access frequency of users by comparing it with access failure information within a specific time. If there exists mismatches in traceback information or the access failure information exceeds a critical value, the access will be identified as an illegal access. Then, the access is immediately interrupted and is recorded as illegal access information. In addition, as an access that is attempted at an unexpected location, which is not registered in the existing user traceback information due to movements of normal users, is presented, the data will be provided after encrypting it for responding illegal accesses due to leaks of OTP. The model presented in this study is safe for authorized users against illegal accesses, which use IP Spoofing in a cloud computing based big data collecting environment, and improves service availabilities.

KEYWORDS: Big data, Big data security, Cloud computing, Computer network, Encryption, Tracebacks

ARTICLE INFO: Received 20 October 2015, Revised 11 December 2015, Accepted 11 December 2015.

1. 서 론

오늘날 빅 데이터 서비스를 위한 클라우드 컴퓨팅 기술은, 우리 사회에 다양한 서비스 제공을 위하여 빠르게 발전하고 있다. 이에 따라 클라우

*Corresponding author is with the Department of Computer Science, Gyeongsang National University, 501, Jinju-daero, Jinju-si, Gyeongsangnam-do, 660-701, KOREA.

E-mail address: jmbae@gnu.ac.kr

드 컴퓨팅 기술을 기반으로 하는 빅데이터의 용량은 TB, PB, ZB까지 급격하게 증가하고 있는 추세이다.[1][2] 그렇지만 이러한 클라우드 컴퓨팅 기반의 빅 데이터 환경은 네트워크를 이용한 공격자들의 집중적인 표적이 되고 있다. 아울러 오늘날 다양하게 변화하는 네트워크 환경에 대한 보안 정책은 아직까지 독립된 단일 보안 대응 시스템을 유지하고 있는 것이 일반적인 상황이다. 그러므로 빠르게 변화하고 있는 네트워크 환경에 능동적으로 대응 가능한 상호 협력 보안 시스템이 필요하다고 할 수 있다. 특히 IP Spoofing 공격은 상호 신뢰 관계에 있는 호스트 정보를 이용하여 불법적인 공격을 시도하기 때문에 클라우드 컴퓨팅 기반의 빅데이터 서비스 환경에서 그 공격 빈도수가 더욱 증가할 수 있다. 게다가 IP Spoofing 공격은 상호 신뢰 호스트 정보 중 IP를 이용하기 때문에 공격 성공을 위하여 반드시 도용한 신뢰 호스트를 무력화 시키는 공격을 유발시킨다. 즉, 네트워크 상에는 동일한 IP가 동시에 두 개 이상 존재할 수 없기 때문이다. 이에 따라 클라우드 컴퓨팅 기술을 기반으로 하는 빅데이터 서비스 환경은 기존의 네트워크 환경 보다 더 많은 IP Spoofing 공격이 빈번할 수 있다. 이러한 이유로 클라우드 컴퓨팅 기반의 빅 데이터 환경은 서비스 가용성과 보안 측면을 동시에 해결할 수 있는 보안시스템을 설계하여야 한다. 본 논문에서는 클라우드 컴퓨팅 기반의 빅데이터 서비스 환경에서 서비스의 안정성과 IP Spoofing을 이용한 불법적인 정보 유출에 대응하기 위하여 다음과 같은 보안 모델을 설계하였다. 먼저 IP Spoofing에 필요한 시스템 자원 고갈 공격 형태가 발생 했는지에 대한 정보를 획득할 수 있도록 하였다.[3] 이는 향후 예비 공격이 발생하면 트레이스 백을 이용하여 공격 탐지에 사용 할 데이터베이스를 구축하기 위함이다. 그리고 기존 정상적인 사용자들은 일반적으로 본인들의 어플리케이션을 쉽게 접근하고 사용한다. 그렇지만 IP Spoofing을 시도한 공격자는 기존 정상 사용자들과 같이 어플리케이션 접근에 실패하는 빈도수가 증가할 수 있다. 이는 접근 정보 자체가 평소 공격자에게 익숙하지 않기 때문이다. 본 논문에서는 정상적인 사용자들의 로그인 성공에 대한 임계치 값을 이용하여 사용자 이용 여부를 검사 정보로 사용하고 있다.

트레이스 백 정보는 본 논문의 사용자 검증 단계에서 경로 분석을 위해 사용한다. 이는 라우팅 과정에 반드시 특정 라우터를 거쳐 출발지에서 목적지까지 도달하기 때문이다.

OTP는 최종 인증 과정의 수행과 이를 이용한 새로운 트레이스 백 정보의 생성과 등록을 위하여 사용한다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문 관련된 연구를 살펴보고, 3장에서는 클라우드 컴퓨팅 기술을 이용한 빅 데이터 환경에서의 보안 대응 모델을 제안하고 그 동작 과정을 설명하였다. 4장에서는 이에 대한 시뮬레이션과 단계별 보안 정책을 수행하였다. 마지막으로 결론과 본 논문의 향후 이용 가능성에 대하여 언급을 하였다.

2. 관련연구

2.1 클라우드 컴퓨팅의 개념

클라우드 컴퓨팅은 분산 처리 기술을 기 반으로 인터넷을 통해 대규모 IT 자원을 임대하고, 사용한 만큼의 요금을 지불하는 컴퓨팅 환경을 의미한다. 그러므로 이러한 환경은 기존의 일반적인 네트워크 환경보다 더욱 강화된 보안 정책을 요구하고 있다.[4] 아울러 이에 따른 개인이나 기업, 공공

기관 등의 보안 시스템에 대한 인식 변화도 필요한 실정이다. 또한 클라우드 컴퓨팅 환경 하에서 발생 가능한 다양하고 불법적인 공격으로부터 중요한 정보 자산을 보호할 수 있는 보안 모델 개발이 절실한 실정이다.[5] [6]

2.2 IP Spoofing 개념

'Spoof'란 단어는 '속이다, 사기치다'는 뜻으로 인터넷 내에서 여러 가지 의미를 지닌다. 'Sniffing'이 타인의 정보를 몰래 훔쳐보는 소극적인 공격인데 반해 'Spoofing'은 아주 적극적이고 고도의 해킹 기술을 보유한 전문적인 해커들의 공격 행위라고 할 수 있다. IP Spoofing이란 자신의 IP를 속여 불법적인 접근을 시도하는 것을 뜻한다. IP Spoofing은 TCP/IP의 구조적인 결함에서 출발한 방법으로 TCP의 시퀀스 번호, 출발지 라우팅 정보, 출발지 IP 주소를 이용하여 <그림 1>과 같이 상대방 호스트가 자신의 호스트를 신뢰하게 만드는 방법이다.[7] 그러므로 이를 이용한 공격은 클라우드 컴퓨팅을 기반으로 하는 빅 데이터 서비스에 대한 불법적인 공격 기법으로 널리 이용될 가능성이 아주 높다고 할 것이다.

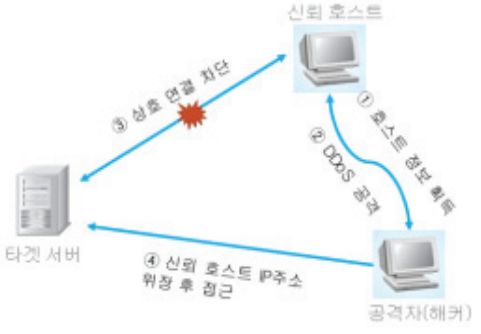

그림 1. IP Spoofing 과정
Figure 1. IP Spoofing process

2.3 트레이스 백 정보의 개념

트레이스 백 정보는 출발지에서 목적지까지 네트워크 경로 분석을 위하여 사용하는 프로그램이다. 즉, 특정 컴퓨터가 네트워크 망을 통하여 최종 목적지에 도착할 때까지 지나가는 각 구간 경로 정보를 기록하는 프로그램이다. 본 논문에서는 불법적인 서비스 접근에 대응하기 위하여 트레이스 백 정보를 이용하여 정상적인 사용자 유무를 판정한다.[8]

2.4 암호화 기법

암호화란 암, 복호화에 사용된 정보를 알지 못하면 해당 내용을 볼 수 없도록 알고리즘을 이용하여 정보를 전달하는 것을 의미한다.

평문이란 송신자가 수신자에게 전달하려는 정보의 내용을 누구라도 그 의미를 알 수 있도록 한 정보이다. 즉, 이러한 평문을 송신자가 암호화 key와 암호화 알고리즘을 적용하여 생성한 것을 암호문이라고 한다. 본 논문에서 암호화 과정은 확신할 수 없는 수신자에게 해당 서비스 자료를 암호화 시켜 전송하고 있다.[9][10]

3. 제안 모델 설계

3.1 제안 모델

본 논문에서 제안하는 불법적인 서비스 접근에 대한 대응 모델은 다음 <그림 2>와 같다.

공격자 H가 시스템 B의 정보를 이용하여 시스템 A에 대하여 IP Spoofing 공격을 시도하는 경우 시스템 A에 등록되어 있는 B의 트레이스 백 정보를 이용하여 1차적인 인증 여부 검사를 실시한다. 만

일 정상적인 사용자의 위치 이동으로 인하여 기존의 사용자 트레이스 백 정보에 등록되어 있지 않은 전혀 다른 위치에서 접근 시도를 하는 경우 OTP를 이용하여 정상 인증 여부를 수행한 후 요청 서비스를 실시한다. 아울러 불법적인 접근으로 판정되면 해당 트레이스 백 정보를 공격 탐지를 위한 상호 공유 트레이스 백 데이터베이스에 등록을 해 둔다.

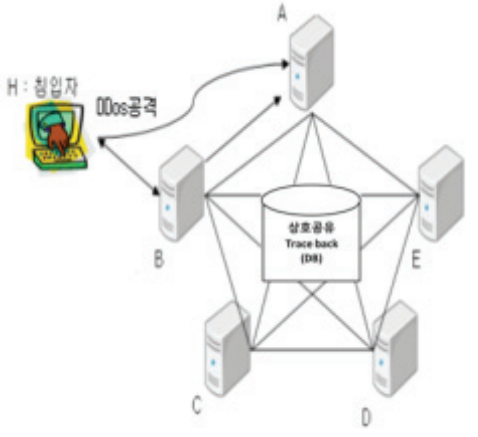

그림 2. 상호 서비스 협력 모델
Figure 2. Cross-service cooperation model

본 논문에서는 자원 고갈 공격이 발생했던 접근 경로 정보, 상이한 경로를 통한 접근 실패 경로 정보, 어플리케이션 접근 실패 경로 정보를 등록해 두었다.

3.2 제안 모델 동작과정

본 논문에서 제안하고 있는 모델의 사용자 접근 처리 과정은 <그림 3>과 같다.

먼저 사용자 접근이 발생하면 자원 고갈 공격 여부를 검사한다. 자원고갈 공격이란 IP Spoofing 공격시 상호 신뢰하고 있는 정상적인 시스템의 동일한 IP를 공유할 수 없기 때문에 신뢰 시스템을 무력화하기 위한 공격이다. 그러므로 이러한 자원 고갈 공격이 발생하면 이들 정보를 IP Spoofing 공격 탐지를 위하여 상호 공유 데이터베이스에 등록해 둔다. 이는 해당 공격자가 첫 번째 공격을 실패할 경우, 클라우드 네트워크를 구성하고 있는 다른 시스템으로 2차, 3차 공격을 시도할 수 있기 때문이다.

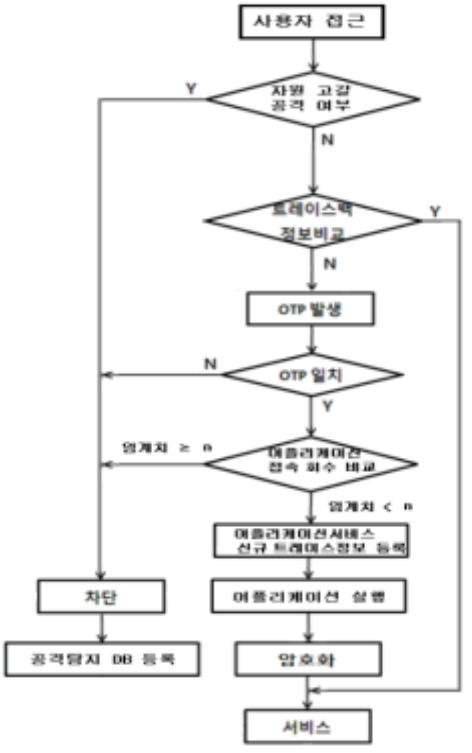

그림 3. 제안 모델의 접근처리 과정
Figure 3. Accessing process in the proposed model

공격자가 첫 번째 공격을 실패한 후 다른 서비스 시스템으로 공격을 시도하면 공격을 당한 해당 시스템은, 첫 번째 시스템에서 상호 공유 데이터베이스에 등록해 놓은 트레이스 백 정보를 참조하여 바로 대응할 수 있도록 하였다. 아

울러 각 서비스 시스템은 자신이 보유하고 있는 상호 접근 가능한 트레이스 백 정보를 이용하여 정상 사용자 접근으로 판정되면 접근을 허용하고 서비스를 실시한다. 일치하지 않는 경우에는 OTP를 발생시켜 접근 여부를 결정한다.

사용자 접근 정보가 상이한 경우는 비정상적인 사용자가 IP Spoofing을 이용하여 접근을 시도하는 경우와, 정상적인 사용자이지만 접근 위치가 기존 등록되어 있는 사용자 접근 위치를 이탈하여 접근하는 경우가 존재할 수 있다. 이러한 경우에는 OTP를 이용하여 접근 경로 정보가 바뀌었다 하더라도 서비스를 지속적으로 유지할 수 있도록 하였다.

마지막으로 OTP 인증 과정을 통과하여 중요 어플리케이션에 대한 접근을 시도하는 경우에는 추가 인증 과정을 거치게 하였다. 이는 정상적인 사용자의 경우 평소 자신의 어플리케이션 이용 과정에 대하여 접근 실패 확률은 거의 없기 때문에 이를 이용하여 추가 인증을 하는 것이다.

만일 어플리케이션 서비스를 위한 접근 실패 횟수가 임계횟수를 넘게 되면 즉각 차단을 하고 이에 대한 트레이스 백 정보를 등록하여 향후 추가 공격에 대응할 수 있도록 하였다. 임계횟수 이내에 로그인을 성공하면 해당 트레이스 백 정보를 자신이 관리하는 시스템의 트레이스 백 정보로 추가 등록하고 향후 접속시 복잡한 인증 과정을 생략할 수 있도록 하였다. 마지막 암호화 단계는 오늘 날 OTP에 대한 공격도 발생하고 있기 때문에, 서비스 가용성과 보안성 모두를 고려하여 요청 자료를 암호화시켜 전송하게 하였다.

4. 실험 및 평가

본 논문에서 사용하고 있는 응용 소프트웨어는 jdk1.8.0_45, Eclipse 4.3.2 SR2, 구현언어는 Java를 사용하였다. 시뮬레이션을 위한 운영 체제는 Windows7 Professional K64비트이고, 시스템 사양은 4GB 메모리를 채택한 Core(TM)i5 2.67GHz System으로 구성하였다. 본 논문은 앞에서 언급했듯이 정상적인 사용자가 기존의 사용자 트레이스 백 정보로 등록되어 있는 위치가 아닌 다른 위치에서 접근을 했을 때 서비스 자료를 암호화하여 해당 정보를 전송한다. 이는 정상적인 접근 정보의 유출로 인하여 불법적인 접근이 발생할 경우까지 고려하여 서비스 가용성과 보안성 모두를 만족시키기 위함이다.

암호화 과정은 클라이언트에서 요구한 서비스 자료를 서버에서 AES 128 암호화 기법을 이용하여 암호화된 자료를 클라이언트로 전송하도록 하였다. 암, 복호화를 위한 키는 패스워드, IP 주소, Hop 개수를 이용하였는데 이는 협력 시스템 상호간 실시간으로 이들 정보를 상호 공유 하고 있기 때문이다.

다음은 암호화키와 복호화키를 이용하여 암호문과 이를 평문으로 전환하는 과정이다.

① 사용자 패스워드에서 먼저 홀수 번째 문자와 짝수 번째 문자를 각각 추출한다.

② IP주소의 각 자리수에 HOP수를 더한 값에서 짝수 번째와 홀수 번째 숫자를 추출한다.

③ 추출된 ①의 각각의 문자에서 같은 위치에 있는 숫자와 ②의 과정에서 생성된 숫자를 더한 후 암호화키를 생성하고 이를 이용하여 암호문을 만든다.

④ 복호화는 이의 역순을 수행한다.

<그림 4>는 빅데이터 환경에서 정상적인 사용자 'ID : 2014214516, Password : 123',자원고갈 공격여부 검증을 통하여 접근이 정상적으로 성공을 한 경우이다.

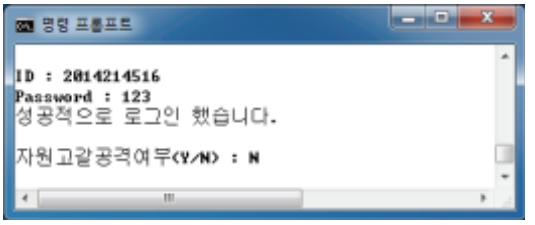

그림 4. 정상적인 사용자 접근
Figure 4. Normal user access

<그림 5>는 트레이스 백 정보를 이용하여 정상 사용자 유무 검사에서 트레이스 백 정보의 불일치로 OTP를 발생시킨 경우이다. 이 경우 OTP를 통한 인증 과정을 거치게 되는데, <그림 5>는 이 과정의 인증에 실패한 경우이다.

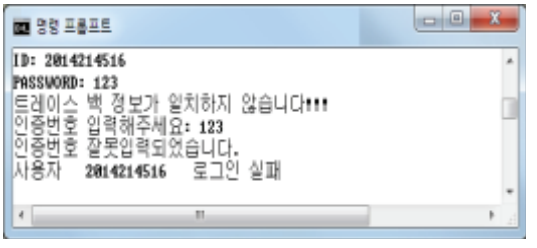

그림 5. 트레이스 백 정보 불일치시 처리과정 결과
Figure 5. Process in a mismatch of traceback information

<그림 6>에서는 트레이스 백 정보가 일치할 경우 요청한 자료에 대하여 암호화 과정 수행 없이 서버에서 클라이언트로 정상적인 서비스 실시를 하는 과정을 보이고 있다.

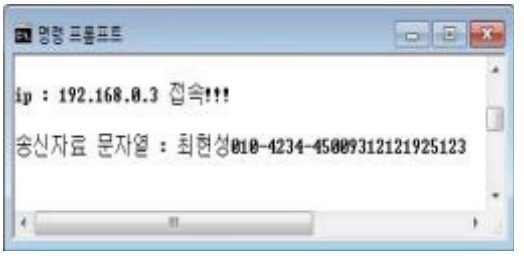

그림 6. 서버에서 정상적인 사용자 자료 송신 과정
Figure 6. Normal data transmitting normal user data in a server

<그림 7>은 <그림 6>의 전송 자료를 클라이언트에서 수신한 것을 보이고 있다.

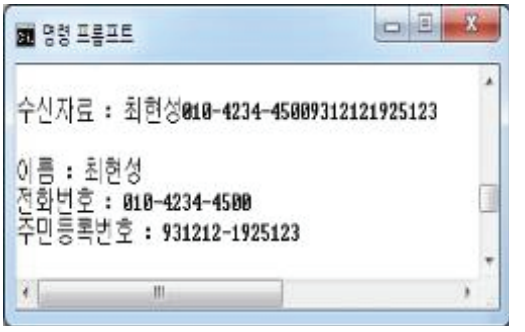

그림 7. 클라이언트에서 정상적인 사용자 자료 수신
Figure 7. Normal user data receiving in a client

<그림 8>은 상이한 경로 일 때 OTP 인증 과정을 통과하여 최종 어플리케이션에 대한 접근을 시도하여 임계횟수 이내인 경우 해당 정보를 서버에서 암호화한 과정을 보이고 있다.

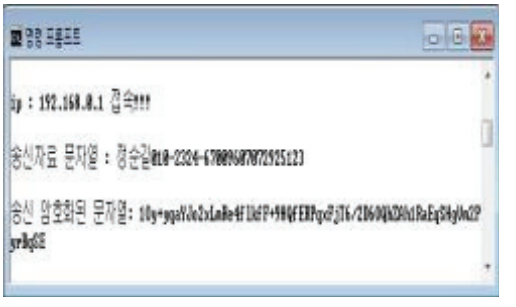

그림 8. OTP 인증 성공 후 서비스 자료 암호화 과정
Figure 8. Encryption process of data in a server

<그림 9>는 <그림 8>의 서버에서 클라이언트로 송신한 암호문을 복호화 시킨 과정을 보이고 있다.

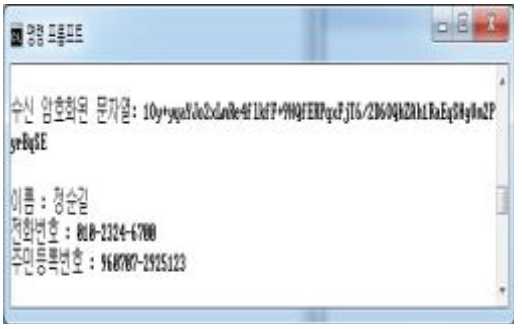

그림 9. 클라이언트에서 암호화 자료 수신
Figure 9. Receiving encrypted data in a client

<그림 10>은 임계치 비교를 통하여 최종 인증 과정을 실패한 경우를 보이고 있다.

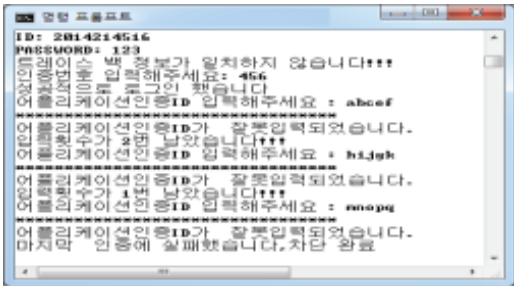

그림 10. 임계치 비교를 통한 최종 인증 과정
Figure 10. Final authentication process through a critical value

References

[1] J.z. Li, and X.M. Liu, *An important aspectt of big data： Data usability,* School of Computer Science and Technology, Harbin Institute of Technology, Harbin 15000 1, pp. 1147~1162, 2013.

[2] Y-Z. Wang, X-L. Jin, and X-Q. Cheng, *Network big data： Present and future,* Key Laboratory of WebData Science&Technology. Institute of Computing Technology, Chinese Academ of Sciences, Beijing 100190, Vol. 36, No. 60, 2013.

[3] S. Curry, E. Kirda, E. Schwartz, W. H. Stewart, and A. Yoran, *Big data fuels intelligence-driven security,* RSA Security Brief, Jan. 2013.

[4] C-S. Yi, and H-J. Yoo, *DDos detecting model of cloud computing environment*, Korea Institute of Infoemation Technology the 2015 KIIT Summer Conference, pp. 4~6, 2015.

[5] O. Chen, and O-n.Deng, *Cloud computing and its key techniques,* Department of Computer Science and Engineering, Shanghai Jiao Tong University,Shanghai 200240, China, Vol. 29, No. 9, pp. 2562~2567, 2009.

[6] J.H. Sun, and K.J. Kim, *Cloud computing in the vulerability analysis for personal information security,* Journal of Information and Security, Vol. 10, No. 4, pp. 77~82, 2010.

[7] H-D. Lee, H-T. Ha, H-C Baek, C-G. Kim, and S-B. Kim, *Efficient detction and defence model against IP spoofing attack through cooperation of trusted hosts,* Journal of the Korea Institute of Information and Communication Engineering, Vol. 24, No. 12, pp. 2649~2656, 2012.

[8] 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.

[9] 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.

[10] J-K. Heo, *Web application authentication system using encipherment and PKI,* Journal of Information and Security, Vol. 8, No. 1, pp. 1~7, 2008.

클라우드 컴퓨팅 환경에서 IP Spoofing 공격 발생시 어플리케이션 접속실패 정보를 이용한 암호화 대응모델 설계

유양, 김상복, 박재홍, 배종민
경상대학교 컴퓨터과학과

요 약

빅 데이터는 일반적으로 많은 양의 정보를 수집한다. 이러한 빅데이터 서비스는 정보를 수집하고 서비스를 받는 과정이 클라우드 컴퓨팅 환경을 기반으로 하고 있다. 그렇지만 이러한 환경은 단일 시스템에서 서비스를 실시하던 환경에 비하여, IP Spoofing을 이용한 불법적인 서비스 접근에 더욱 쉽게 노출될 가능성이 높다고 할 것이다. 본 논문에서는 클라우드 컴퓨팅 환경에서 불법적인 서비스 접근에 대응하기 위하여 트레이스 백 정보를 이용하여 정상적인 사용자 유무를 판정한다. 그런 다음 해당 사용자의 단위 시간내 접속 실패 정보를 비교하여 정상적인 빈도수이면 서비스를 실시한다. 만일 트레이스 백 정보가 일치하지 않거나 접속 실패 정보가 임계치를 넘게 되면 불법적인 사용자 접근으로 판정하고 해당 접근을 즉각 차단한 후 불법 접근 정보로 등록 해 둔다. 또한 정상적인 사용자의 위치 이동으로 인하여 기존의 사용자 트레이스 백 정보에 등록되어 있지 않은 전혀 다른 위치에서 접근 시도를 하는 경우, OTP를 이용하여 정상인증 여부를 수행한 후 해당 서비스 자료를 암호화 시켜 전송한다. 이는 오늘 날 OTP 유출로 불법적인 자료 접근이 발생하고 있기 때문에 이에 대응하기 위함이다. 본 논문은 클라우드 컴퓨팅 기반의 빅 데이터 자료 수집 환경에서 IP Spoofing을 이용한 불법적인 접근에 대하여 인가된 사용자별로 안정적이면서, 서비스 가용성을 향상시킨 모델이라고 할 수 있다.

Yang Liu received the Master´s degree in the Department of Computer Science from Gyeongsang National University in 2015. His current research interests include network architecture, bigdata security, network security.

E-mail address: a2633558a@naver.com

Sang Bok Kim received the Ph.D. degree in the Department of Electronics Engineering from Chung-ang University in 1989. He was a director in the Department of Education Information Computer Center at The Gyeongsang National University from 2007 to 2010. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1984. He has been a researcher in the Computer Data Communication Research Institute at The Gyeongsang National University since 1984. His current research interests include computer network and security, computer system architecture. He is a member of the KKITS.

E-mail address: sbkim@gnu.kr

Jae Heung Park received the Ph.D. degree in the Department of Computer Engineering from Chung-ang University in 1989. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1983. He has been a researcher in the Software

Engineering Research Institute at The Gyeongsang National University since 1984. His current research interests include computer network and security, S/W Reliability. He is a member of the KKITS.

E-mail address: pjh@gnu.ac.kr

Jong Min Bae received the Ph.D. degree in the Department of Computer and Statistics from Seoul National University in 1995. He has been a professor in the Department of Computer Science at Gyeongsang National University since 1984. His current research interests include programming languages, computer education, and compilers.

E-mail address: jmbae@gnu.ac.kr