한국정보전자통신기술학회논문지(jkiiect)'17-12, Vol.10 No.6
논문 17-12-06-580 http://dx.doi.org/10.17661/jkiiect.2017.10.6.580

클러스터링 환경에 대한 IP 스푸핑 공격 발생시 라우팅 패턴에 기반한 단계별 서비스 암호화 모델

백 용 진*, 정 원 창*, 홍 석 원*, 박 재 흥**

A step-by-step service encryption model based on routing pattern in case of IP spoofing attacks on clustering environment

Yong-Jin Baek*, Won-Chang Jeong*, Suk-Won Hong*, Jae-Hung Park**

요 약 빅데이터 서비스 환경 구축과 서비스에는 클라우드 기반의 네트워크 기슬과 정보 접근의 효율성 개선을 위한 클러스터링 기술이 함께 요구된다. 이러한 클라우드 기반의 네트워크와 클러스터링 환경은 다양하고 가치있는 정보를 실시간으로 제공 할 수 있기 때문에, 불법적인 접근을 시도하는 공격자들의 집중적이 표적이 될 수 있다. 특히 IP 스푸핑을 시도하는 공격자들은 클러스터링을 구성하고 있는 상호 신뢰 호스트들의 정보를 분석하여, 클러스터 내에 존재하는 시스템으로 직접 공격을 시도할 수 있다. 그러므로 불법적인 공격에 대한 빠른 탐지와 대응이 필요하며, 기존의 단일 시스템에서 구축하여 운용하는 보안시스템 보다 강화된 보안정책이 요구된다고 할 것이다. 본 논문은 이러한 네트워크 환경에서의 불법적인 공격 발생에 능동적인 대응 및 효율적인 정보 서비스가 가능 할 수 있도록 라우팅 패턴 변화를 추적하여 탐지 정보로 활용하였다. 아울러 탐지 과정에서 발생하는 라우팅 정보에 기반한 단계별 암호화를 통하여 재설정을 위한 잦은 정보 서비스의 단절이 발생하지 않으면서 안정적인 서비스 정보의 관리가 가능하도록 하였다.

Abstract The establishment of big data service environment requires both cloud-based network technology and clustering technology to improve the efficiency of information access. These cloud-based networks and clustering environments can provide variety of valuable information in real-time, which can be an intensive target of attackers attempting illegal access. In particular, attackers attempting IP spoofing can analyze information of mutual trust hosts constituting clustering, and attempt to attack directly to system existing in the cluster. Therefore, it is necessary to detect and respond to illegal attacks quickly, and it is demanded that the security policy is stronger than the security system that is constructed and operated in the existing single system. In this paper, we investigate routing pattern changes and use them as detection information to enable active correspondence and efficient information service in illegal attacks at this network environment. In addition, through the step-by -step encryption based on the routing information generated during the detection process, it is possible to manage the stable service information without frequent disconnection of the information service for resetting.

Key Words : Big data, Cloud Computing, DDoS, Encryption, IP Spoofing, Security, Traceback

1. 서 론

정보통신 기술의 급격한 발전은 우리 생활 전반에 다양한 서비스를 온라인으로 제공하고 있다. 그러므로 정보의 상호 교환 과정에 제공되는 서비스 자료에 대

*Department of Computer Science, Gyeongsang National University
**Corresponding Author : Department of Computer Science, Gyeongsang National University(pjh@gnu.ac.kr)
Received November 30, 2017 Revised December 14, 2017 Accepted December 22, 2017

한 보안 기능이 더욱 요구되는 상황이다[1,2].

정보의 불법적인 접근에 대응할 수 있는 기술에는 인증 기법, 탐지 기법, 암호화 기법이 대표적이라고 할 수 있다[3,4]. 하지만 이러한 대응 기법들은 빠르게 발전하고 있는 다양한 공격에 신속한 대응이 어려운 실정이다. 또한 클라우드와 클러스터링 기반의 빅 데이터 서비스 환경은 고도의 공격기술을 보유하고 있는 공격자들로부터 집중적인 공격 대상이 될 수 있다. 특히 IP 스푸핑 공격은 상호 신뢰 관계에 있는 호스트의 정보를 이용하여 불법적인 공격을 시도하는 공격이다. 그러므로 클라우드 및 클러스터링을 기반으로 하는 환경에서는 이러한 신뢰 관계를 이용한 공격이 빠르게 증가할 수 있다[5,6,7].

본 논문은 클라우드 및 클러스터링 환경에서 불법적인 접근의 빠른 탐지와 서비스 지속성 향상을 위하여 라우팅 과정에 존재하는 라우터들의 IP 패턴 변화를 분석하여 암호화 정보로 사용하였다. 그 다음 이를 기반으로 기존 대응 기법에 존재하는 잦은 서비스 단절 문제를 개선하였다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 관련 연구를 살펴보고, 3장에서는 트레이스백 정보를 이용한 정상적인 IP에 대한 변이를 분석하여 단계별 암호화를 수행할 수 있는 모델을 설계하였다. 그 다음 4장에서는 패턴 변화가 존재하는 연결에 대하여 단계별 암호화 과정을 수행하도록 하였다. 마지막 결론 부분은 본 논문의 향후 이용 가능성에 대한 언급을 하였다.

2. 관련연구

Spoofing이라는 것은 '속이다'라는 의미를 나타내는데, IP 스푸핑은 상호 신뢰호스트의 IP주소를 이용하여 또 다른 신뢰 호스트를 공격하는 방법이다.

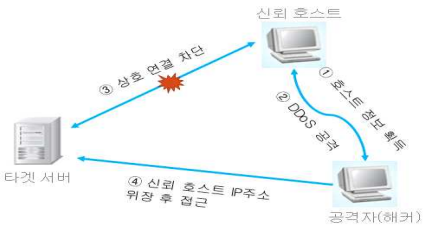

그림 1. IP 스푸핑 공격의 예
Fig. 1. Examples of IP spoofing attacks

(그림 1)과 같이 신뢰호스트가 공격자의 위장된 IP를 신뢰하도록 하는 공격 기법으로, 그 과정은 먼저 공격자가 타겟 서버를 공격하기 위해 타겟 서버가 신뢰하는 임의의 신뢰호스트 IP 정보를 획득한다. 그 다음 해당 호스트로 DoS나 DDoS 등 자원 고갈 공격을 시도하여 해당 신뢰호스트를 다운시킨다. 그 후 타겟 서버와 신뢰호스트의 상호 연결 상태가 단절되면, 공격자는 해당 신뢰호스트의 IP주소를 위장하여 타겟 서버에 대한 불법적인 접속을 시도한다. 아울러 IP 스푸핑 기법은 공격의 특성상 향후 클라우드 환경에서 집중적으로 발생할 가능성이 아주 높다. 클라우드 컴퓨팅의 의미는 네트워크상에 존재하는 하드웨어 소프트웨어 등의 컴퓨팅 자원을 이용자의 요구에 따라 실시간으로 소프트웨어, 플랫폼, 인프라 등 IT자원을 필요한 만큼 서비스 받고, 이에 대한 사용요금을 지급하는 방식의 네트워크 구성을 의미한다. 그러므로 빅 데이터 환경 구축에는 클라우드 컴퓨팅 기술이 반드시 필요한 기반기술이라고 할 수 있다.

IP 스푸핑을 탐지할 수 있는 기존의 탐지 방식에는 접근을 요청하는 시스템으로 트레이스백 정보를 요청한 후, 이를 분석하여 정상적인 접근 여부에 대한 판정을 하는 방식이 있다.

트레이스백이란 네트워크 경로 분석을 하기 위한 것으로 네트워크 과정 중 출발지로부터 목적지까지 경유하는 각 구간의 라우터 정보를 기록하는 프로그램이다.

기존의 논문에는 트레이스백을 통하여 수집한 경로 정보를 단순 비교하는 방식을 취하고 있다[8]. 그렇지만 트레이스백 정보의 단순 비교는 정상적인 사용자를 공격자로 판정하는 오류가 발생할 수 있으며 이로 인한 서비스 단절이 빈번하게 발생할 수 있다. 오탐율을 개선하기 위한 기존의 논문에는 OTP를 이용한 재인증 과정을 수행하는 방법이 있다. 하지만 트레이스백 정보의 분석 후 재인증을 위한 OTP를 전송하는 방식은 라우팅 과정에 존재하는 라우터들의 IP 변동이 존재할 때 마다 OTP를 전송하기 때문에 이에 대한 오버헤드를 초래할 수 있다[9,10,11].

본 논문에서는 OTP의 잦은 전송으로 발생할 수 있는 인증 과정의 오버헤드를 감소시키기 위하여, 트레이스백 정보의 변화에 따른 단계별 암호화 과정을 수

행하여 이를 개선하였다. 암호화란 중요한 정보를 권한이 없는 일반 사용자가 읽을 수 없도록 하는 기법이다. 빅데이터 환경에서는 불법적인 접근을 통하여 다양한 자료를 수집한 후 가치 있는 새로운 정보를 생성할 수 있기 때문에 이를 위한 암호화 과정은 반드시 필요하다고 할 것이다. 본 논문에서는 트레이스백 정보를 수집하여 정상적인 접근자와 IP 스푸핑을 시도하는 공격자를 분석한 후 단계별 암호화와 복호화 정보로 사용하였다.

복호화란 암호화된 자료를 권한이 있는 특정 사용자가 읽을 수 있는 형태로 복원시키는 과정을 의미한다. 그러므로 다양한 정보 교환이 이루어지는 네트워크 환경에서는 이러한 암호화/복화 과정을 이용하여 서비스 단절 보다는 서비스 지속성을 향상시켜 실시간 서비스를 개선할 수 있어야 한다.

본 논문에서는 이러한 클라우드 기반의 빅 데이터 환경에서 IP 스푸핑 공격에 대한 방대한 자료의 보안 관리를 위하여, 불법적인 접근에 대한 효율적인 방어와, 서비스 지속성을 향상시킬 수 있도록 클러스터링을 구성하는 시스템들이 집단적인 방어 시스템을 구축하여 실시간으로 공격 정보를 공유할 수 있도록 하였다.

3. 제안 모델 설계

3.1 제안 모델

기존의 모델들이 일반적으로 불법적인 접근에 대한 연결을 단절시키는데 비하여 본 논문에서 제안하는 모델은 서비스 지속성을 향상 시킨 모델이라고 할 수 있다. 기존 공격탐지 모델의 경우 트레이스백 정보를 비교한 후 해당 정보가 상이할 경우 OTP를 발생시켜 연결에 대한 재설정을 요구한다. 즉, 트레이스백 정보가 완전하게 일치하지 않으면 매 번 OTP를 통한 재설정 과정을 요구하게 된다. 본 논문에서는 이러한 문제점을 개선하기 위하여, 상이한 경로 정보가 탐지되면 해당 시점부터 암호화 과정을 3회에 걸쳐 단계적으로 실시한다. 3회의 암호화 과정에서 각각 정상적으로 복호화 과정을 수행할 경우 해당 경로 정보를 정상적인 사용자로 분류한 후 공격 탐지를 위한 데이터베이스에 등록해 둔다. 이는 향후 동일한 경로에서 접근할 경우 추가적인 암호화 과정이 발생하지 않도록 하기 위함이다.

3.2 제안 모델 동작과정

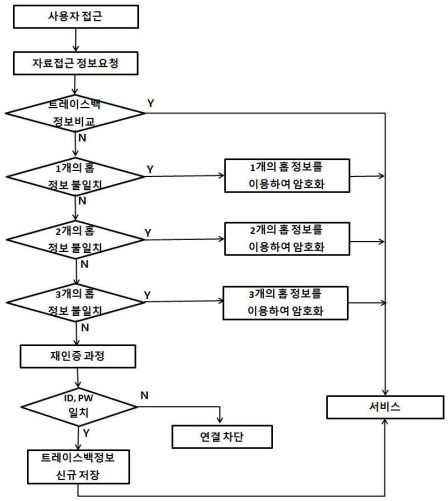

그림 2. 제안모델 동작 과정
Fig. 2. Proposed model operation process

본 논문에서 제안하는 모델의 동작 과정은 (그림 2)와 같다. 먼저 사용자 접근이 발생한 후 자료에 대한 접근 요청이 발생하면 다음 과정을 수행한다.

STEP 1. 서버에서 보유하고 있는 경로 정보 중 자료접근 요청자의 IP와 일치하는 트레이스백 정보를 선택하여 순차적으로 비교해 나간다.

1-1. 트레이스백 정보의 비교 과정에서 해당 경로 정보가 완전하게 일치하면 서비스 작업을 바로 수행한다.

STEP 2. 트레이스백 정보의 비교과정에서 상이한 경로 정보가 한 개만 존재할 경우 기존의 정상적인 경로로 등록해 둔 동일한 홉의 정보 중 상호 약속한 한 개 홉의 정보를 암호화/복호화 키 값으로 하여 암호화 과정을 수행하고 이를 클라이언트로 전송한다.

2-1. 서버로부터 요청 자료를 수신한 클라이언트는 자신이 보유하고 있는 홉 정보 중 서버와 미리 약속한 IP 주소를 이용하여 해당 자료를 복호화 시킨다.

STEP 3. 트레이스백 정보의 비교과정에서 상이한 경로 정보가 두 개 존재할 경우 기존의 정상적인 경로로 등록해 둔 동일한 홉의 정보 중 상호 약속한 두 개 홉의 정보에서 암호화/복호화 키 값을 추출하여 암호

화 과정을 수행하고 이를 클라이언트로 전송한다.

3-1 서버로부터 요청 자료를 수신한 클라이언트는 자신이 보유하고 있는 홉 정보 중 서버와 미리 약속한 IP 주소를 이용하여 해당 자료를 복호화 시킨다.

STEP 4. 트레이스백 정보의 비교과정에서 상이한 경로 정보가 세 개 존재할 경우 기존의 정상적인 경로로 등록해 둔 동일한 홉의 정보 중 상호 약속한 세 개 홉의 정보에서 암호화/복호화 키 값을 추출하여 암호화 과정을 수행하고 이를 클라이언트로 전송한다.

4-1 서버로부터 요청 자료를 수신한 클라이언트는 자신이 보유하고 있는 홉 정보 중 서버와 미리 약속한 IP 주소를 이용하여 해당 자료를 복호화 시킨다.

STEP 5. 트레이스백 정보의 비교과정에서 상이한 경로 정보가 네 개 이상 존재할 경우 재인증 과정을 수행한다.

5-1 재인증 과정에는 ID, PASSWD, OTP를 이용한다.

5-2 재인증 과정을 정상적으로 수행한 경우 접근자 정보가 신규로 발생한 것으로 간주하여 이를 정상적인 트레이스백 정보로 저장 해 둔다.

5-3 재인증 과정을 정상적으로 수행하지 못한 경우에는 이를 즉각 차단하고, 해당 정보를 공격자 정보에 신규 등록을 한다.

본 논문에서 트레이스 백 정보가 네 개 이상 일치하지 않을 경우 계속적인 암호화/복호화는 전체 서비스 성능을 저하시킬 수 있기 때문에 바로 재인증 과정을 수행하도록 하였다.

본 논문은 서비스 가용성 향상을 위하여 단계적으로 3회의 암호화 및 복호화 과정을 수행하고 있다. 그러므로 기존의 논문에서 발생하는 트레이스백 정보의 비교분석 과정에서 나타나는 OTP의 남발이나 연결 단절 문제를 감소시켜 지속적인 서비스 상태를 유지시킬 수 있다,

4. 실험 및 평가

4.1 시뮬레이션 환경

본 논문에서 제안하는 클라우드 기반의 네트워크 환경에 대한 보안 시뮬레이션 환경은 다음과 같다. 먼저 사용된 응용 소프트웨어는 jdk1. 8.0_45, Eclipse 4. 3.2 SR2, 구현언어는 Java를 사용하였다. 시뮬레이션을 위한 운영 체제는 Wind ows 7 Professional K64 비트이고, 시스템 사양은 8GB 메모리를 채택한 Core (TM)i5 2.67GHz Sys tem으로 구성하였다.

그림 3. 트레이스 백 정보가 일치하는 경우
Fig. 3. Traceback information matching case

그림 3은 트레이스 백 정보가 모두 일치하는 경우 요청자료에 대하여 정상적인 서비스를 수행하는 것을 보이는 것이다

그림 4. 트레이스 백 정보가 4회 이상 불일치하는 경우
Fig. 4. Examples of the traceback information is at least four times a mismatch

그림 4는 트레이스 백 정보가 4회 이상 불일치하지만 재인증 과정을 통하여 정상적인 사용자로 판단되어 해당 서비스를 정상적으로 수행하고 있는 것을 보여주는 것이다.

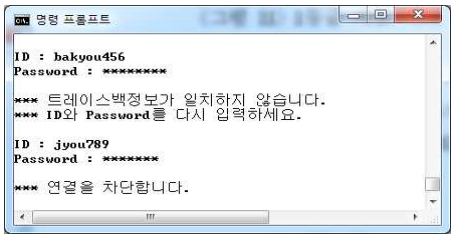

그림 5. 서버에서 재인증 과정이 실패한 경우
Fig. 5. Reauthentication process failed on server

그림 5는 트레이스 백 정보가 4회 이상 불일치하여

재인증 과정을 수행했지만, 인증에 실패하여 연결을 차단한 결과를 보여주는 것이다.

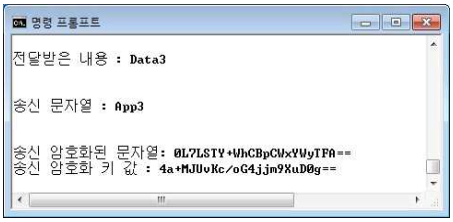

그림 6. 1개의 홉이 불일치한 경우 서버 처리 과정
Fig. 6. Server processing when one hop is mismatched during traceback analysis

그림 6은 특정 트레이스 백 정보 중 한 개가 일치하지 않을 경우, 클라이언트에서 요청한 'App3'이라는 자료를 해당 홉에 대응하는 서버의 트레이스백 정보를 이용하여 이를 암호화 시킨 후 클라이언트로 전송하는 과정을 보여주고 있다.

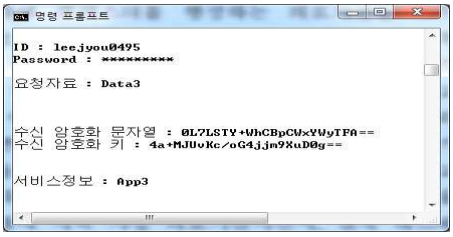

그림 7. 1개의 홉이 불일치한 경우 클라이언트에서 처리 과정
Fig. 7. Client processing when one hop in the traceback information is mismatched

그림 7은 그림 6에서 암호화 시킨 결과를 서비스 요청을 한 정상적인 클라이언트가 수신하여 상호 약속한 복호화 키를 이용하여 평문으로 복호화 시킨 결과이다. 그림 7에서 보면 'App3'이 정상적으로 서비스가 된 것을 알 수 있다.

이상의 그림 6, 그림 7에서와 같이 트레이스백 정보가 두 개, 세 개 까지 상이할 경우 해당 홉의 정보가 증가하기 때문에 암호화 강도를 지속적으로 높여 나갈 수 있다. 아울러 암호화 강도가 높아지더라도 클라이언트에는 이미 해당 홉에 해당하는 약속한 경로 정보가 존재하기 때문에 정상적인 접속자라면 이를 쉽게 복호화 시킬 수 있다.

5. 결 론

본 논문은 향후 빅데이터 서비스 환경 구축에 반드시 필요한 클라우드 기반의 네트워크 환경에 대한 보안 모델을 제시한 것이다. 또한 상호 연관된 서비스 자료의 집중적인 수집이 발생할 수 있는 클러스터링 환경에도 적용 가능한 모델이라고 할 수 있다.

네트워크를 통한 정보의 수집과 서비스 과정은 보안 정책과 서비스 가용성 측면에서 상호 반비례적인 성격을 나타낸다. 즉, 보안 정책을 강화시키면 서비스 가용성을 저하시키고, 서비스 가용성을 향상시키면 보안 정책에 대한 문제점을 보다 더 노출시킬 수 있기 때문이다.

기존의 논문들은 접근 요청이 발생하면 트레이스 백을 실행하여 상이한 경로 정보가 탐지될 경우 IP 스푸핑으로 판정하고 연결에 대한 단절이나 OTP를 이용한 재인증 과정을 수행한다. 트레이스 백 정보를 기반으로 하는 이러한 대응 방식은 공격에 대한 방어적인 차원에서는 보다 안정적이라고 할 수 있다. 그렇지만 상이한 경로 정보가 탐지될 때 마다 매 번 이러한 과정을 수행하게 되면 서비스 가용성은 현저히 저하될 수밖에 없다. 본 논문은 이러한 문제를 해결하기 위하여 상이한 경로 정보가 발생할 경우 즉각적인 서비스 단절보다는 단계별로 암호화 강도를 높여 서비스 작업을 수행하기 때문에 서비스 가용성을 향상시킬 수 있었다.

IP 스푸핑을 시도하는 공격자들은 클라우드 기반의 네트워크에 대하여 변화된 공격을 시도할 수 있다. 그러므로 클라우드나 클러스터링을 구성하고 있는 시스템 환경에서는 보안정책을 집단적인 공격 대응 방식으로 재구축 할 필요가 있다. 향후 연구 과제로는 집단적인 보안 네트워크에서 요구하는 공격 정보의 공유와 이를 기반으로 하는 공격 탐지 기술이 함께 연구되어야 할 것으로 본다.

REFERENCES

[1] C-C. Park, G-H. Park, S-H. Kim, and S-H. Koh, "The proposal of evaluation measure from hospital information system : The case study of C national university hospital in

Korea", Journal of The Korea Knowledge Information Technology Systems, Vol. 2, No. 2, pp. 69-77, 2007.

[2] J-H. Choi, "Analysis of changes in the muscle activity and fatigue of the erector spinae using IT convergent type medical equipment", Journal of Knowledge Information Technology and Systems, Vol. 10, No. 6, pp. 665-673, 2015.

[3] S-K. Park, "A study on the regional differences of telemedicine and digital divide", Journal of the Korean Geographical Society, Vol. 50, No. 3, pp. 325-338, 2015.

[4] J-J. Hoon, "A study on the vulnerability and corresponding technique trends of the cloud computing service", Convergence security journal, Vol 13, No. 6, pp. 17~24, 2013. 4.

[5] J-K. Park, "A study on measures to active cultural contents service in big data age", Vol. 20, No. 1, pp. 324-334, Mar. 2014.

[6] Q. Miao, "When intelligence meeting wity big data : Review and perceptions of big Data'S hotspot intelligence tracking", Institute of Scientific & Technical Information of Shanghai,Shanghai 200031, No. 5, Serial No. 187, 2013.

[7] S-Y. Kim, J-I. Lim, and K-h. Lee, "A study on the security policy improvement using the big data, Korea University", Graduate School of Information Security, Vol. 23, No. 5, pp. 969-976, 2013, http://dx.doi.org/10.13089/JKIISC.2013.23.5.96, 2013.

[8] M-H. Kim, B-H. Chul, H-S. Won, and J-H. Park, "An Encrypted Service Data Model for Using Illegal Applications of the Government Civil Affairs Service under Big Data Environments", Convergence security journal, Vol 15, No. 7, pp. 31~38, 2015. 12.

[9] S. Bellovin, M. Leech, and T. Taylor, "ICMP Traceback message", IETF, draft-ietfitrace-04, Feb. 2003.

[10] Y-Y. Mu, H-C. Baek, J-Y. Choi, W-C. Jeong, and S-B. Kim, "A proposal of a defense model for the abnormal data collection using trace back information in big data environments", Journal of Knowledge Information Technology and Systems, Vol. 10, No. 2. pp. 753-162, 2015.

[11] S-P. Huh, D-S. Lee, K-N. Kim, "A Study on The Improvement of User Authentication using the Facial Recognition and OTP Technique in the Mobile Environment", Convergence security journal, Vol 11, No. 3, pp. 75~84, 2011. 6.

저자약력

백 용 진(Yong-Jin Baek) **[학생회원]**

- 2015년 2월 경남과학기술대학교 컴퓨터공학과 학사
- 2017년 11월 경상대학교 컴퓨터과학과 석사 과정

<관심분야> 네트워크보안, 빅데이터보안, 사물인터네보안, 암호화

정 원 창 (Won-Chang Jeong) **[정회원]**

- 1996년 2월 경상대학교 컴퓨터과학과 학사
- 1999년 8월 경상대학교 컴퓨터과학과 석사
- 2009년 2월 경상대학교 컴퓨터과학과 박사
- 2001년 ~ 현재 진주보건대학교 복지행정계열 교수

<관심분야> 네트워크보안, 센서네트워크

홍 석 원 (Suk Won Hong) **[정회원]**

- 2003년 2월 경남과학기술대학교 컴퓨터공학과 학사
- 2006년 2월 경상대학교 컴퓨터과학과 석사
- 2011년 2월 경상대학교 컴퓨터과학과 박사
- 1999년 4월 ~ 현재 : 경남도립 거창대학

<관심분야> 네트워크보안, 빅데이터

박 재 홍 (Jae-Hung Park) **[정회원]**

- 1978년 2월 충북대학교 수학교육과 학사
- 1980년 9월 중앙대학교 전자계산학과 석사
- 1989년 8월 중앙대학교 전자계산학과 박사
- 1984년 4월 ~ 현재 경상대학교 컴퓨터과학과 교수

<관심분야> 컴퓨터보안, 암호화, 소프트웨어공학