https://doi.org/10.33778/kcsa.2019.19.5.047

# 클라우드 환경에서 네트워크 가용성 개선을 위한 대칭키 암호화 기반 인증 모델 설계

백용진*, 홍석원**, 김상복***


## 요 약

네트워크를 통한 정보의 공유는 오늘날 클라우드 서비스 환경으로 발전하여 그 이용자수를 빠르게 증가시키고 있지만 네트워크를 기반으로 하는 불법적인 공격자들의 주요 표적이 되고 있다. 아울러 공격자들의 다양한 공격 기법 중 IP 스푸핑은 그 공격 특성상 일반적으로 자원고갈 공격을 수반하기 때문에 이에 대한 빠른 탐지와 대응 기법이 요구 된다. IP 스푸핑 공격에 대한 기존의 탐지 방식은 연결 요청을 시도한 클라이언트의 트레이스 백 정보 분석과 그 일치 여부에 따라 최종적인 인증과정을 수행 한다. 그렇지만 트레이스 백 정보의 단순 비교 방식은 서비스 투명성을 요구하는 환경에서 빈번한 False Positive로 인하여 과도한 OTP 발생을 요구할 수 있다. 본 논문에서는 이러한 문제를 개선하기 위해 트레이스 백 정보 기반의 대칭키 암호화 기법을 적용하여 상호 인증 정보로 사용하고 있다. 즉, 트레이스 백 기반의 암호화 키를 생성한 후 정상적인 복호화 과정의 수행 여부로 상호 인증이 가능하도록 하였다. 아울러 이러한 과정을 통하여 False Positive에 의한 오버헤드도 개선할 수 있었다.


# The Design of Authentication Model based on Symmetric Key Encryption for Improving Network Availability in Cloud Environment

Yong-Jin Baek*, Suk-Won Hong**, Sang-Bok Kim***


## ABSTRACT

Network-based sharing of information has evolved into a cloud service environment today, increasing its number of users rapidly, but has become a major target for network-based illegal attackers.. In addition, IP spoofing among attackers' various attack techniques generally involves resource exhaustion attacks. Therefore, fast detection and response techniques are required. The existing detection method for IP spoofing attack performs the final authentication process according to the analysis and matching of traceback information of the client who attempted the connection request. However, the simple comparison method of traceback information may require excessive OTP due to frequent false positives in an environment requiring service transparency. In this paper, symmetric key cryptography based on traceback information is used as mutual authentication information to improve this problem. That is, after generating a traceback-based encryption key, mutual authentication is possible by performing a normal decryption process. In addition, this process could improve the overhead caused by false positives.


**Key words : Big data, Security, Cloud Computing, Encryption, Traceback, Telemedicine, IPSpoofing, DDoS**

접수일(2019년 10월 5일), 수정일(1차: 2019년 12월 27일), 게재확정일(2019년 12월 30일)

* 경상대학교 컴퓨터과학과
** 경남도립거창대학
*** 경상대학교 컴퓨터과학과(교신저자)

# 1. 서 론

일반적인 네트워크 환경은 다양한 빅데이터(Big Data) 서비스를 제공하는데 있어 그 한계성을 보이고 있다. 그러므로 이를 개선하기 위한 새로운 네트워크 서비스로 클라우드(Cloud) 환경 구축을 요구하고 있다. 그렇지만 네트워크 환경이 다양해질수록 불법적인 공격자들은 기존의 공격기법에 새로운 공격기법을 응용하여 불법적인 접근을 지속적으로 시도하고 있다.

특히 IP 스푸핑(Spoofing) 공격은 서비스 요청자와 제공자의 정상적인 상호 인증에 사용되는 IP 주소를 속여 공격을 시도하는 기법이다[1].

클라우드 서비스를 수행중인 서버의 경우 서비스 안정성 보장을 위해 적극적인 보안 시스템을 운영하고 있다. 이에 대응하여 불법적인 접근을 시도하는 공격자들은 클라우드 서버에 대한 직접적인 공격대신 클라우드 서버에서 상호 신뢰하고 있는 시스템의 IP 정보를 이용하여 우회 공격을 시도한다.

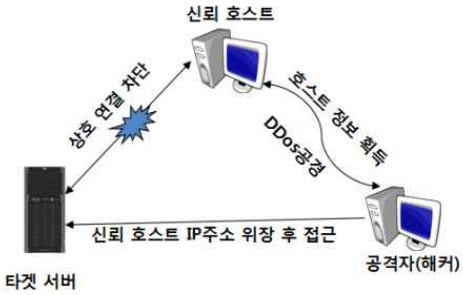
IP 스푸핑은 상호 신뢰 관계에 있는 시스템의 접근 정보를 이용하여 불법적인 연결을 시도하기 때문에 클라우드 기반의 빅데이터 서비스 환경에서는 그 공격 빈도수가 더욱 증가할 수 있다. 아울러 이러한 IP 스푸핑 공격에 대한 기존 탐지 방식에는 트레이스 백(Traceback)정보를 단순 비교한 후 정상적인 인증 과정을 수행하는 방식이 있다[2][3]. 이와 함께 불법적인 서비스 접근을 방지하기 위한 대응기술로는 일반적으로 탐지 기법 및 암호화 기법이 존재하며, 이들은 다양한 네트워크 환경과 해당 서비스의 특성에 따라 단일 또는 둘 이상의 기법을 조합하여 복합적으로 운용하고 있다[4].

클라우드 기반의 네트워크 환경에 대한 IP 스푸핑 공격이 발생할 경우, 유출되는 다양한 정보로 인하여 심각한 보안 사고를 초래할 수 있다. 그러므로 기존의 트레이스 백 정보의 단순 비교 방식에는 그 한계성이 존재하며, 이를 개선하기 위한 새로운 보안 시스템 구축이 필요하다.[5-7]. 그렇지만 이러한 개선 기법도 OTP의 빈번한 생성과 인증 과정의 수행으로 네트워크 질 저하를 초래할 수 있으며, False Positive 문제를 발생시킬 수 있다. 그러므로 본 논문에서는 트레이스 백 정보 기반의 대칭키 암호화 알고리즘 방식을 적용하여 암호화/복호화 과정의 정상 수행 여부를 통해 기존의 인증 방식에서 발생 할 수 있는 오버헤드를 감소시킬 수 있었다.

# 2. 관련연구

## 2.1 IP 스푸핑

다음 (그림 1)은 일반적인 IP 스푸핑 기법을 도식화 해 놓은 것이다. 네트워크 기반의 공격에는 다양한 기법들이 존재하고 있지만, IP 스푸핑은 적극적이면서 고도의 해킹 기술을 보유한 전문 해커들이 주로 사용하는 공격 기법이다[8]. 특히 클라우드 서비스를 지원하는 네트워크 환경은 이들 공격자들의 집중적인 표적이 될 수 있기 때문에 서비스 가용성을 향상시킬 수 있는 대응 기법이 요구된다.




(그림 1) IP 스푸핑 과정

## 2.2 암호화

대칭키 암호화 알고리즘의 대표적인 방식으로 DES 알고리즘이 존재하지만, 이를 복호화하기 위한 공격자들의 공격 기술 또한 발전하고 있기 때문에 강화된 암호화 기능이 필요하다.

AES(Advanced Encryption Standard)는 대칭키 기법의 미국 연방 표준 알고리즘으로서 기존의 온 DES 암호화 알고리즘을 대체할 수 있는 차세대 암호화 알고리즘이다. AES 암호화 암고리즘은 암호화/복호화 과정에 사용하는 키의 길이에 따라 AES-128, AES-192, AES-256으로 구분하며, 대칭키의 길이와 블록의 크기에 따라 10, 12, 14 라

운드 과정을 수행한다[9][10][11].

### 2.3 트레이스 백의 의미

일반적인 특정 송신자 및 수신자의 네트워킹 과정에는 경유 라우터들이 존재하는데 트레이스 백이란 이들 정보를 분석하기 위한 프로그램이다. 상호 송/수신을 수행하는 특정 시스템들의 패킷은 최종 목적지까지 도달하기 위해 다수의 라우터를 경유하게 되는데, 이들 구간에 존재하는 IP를 획득하여 패킷의 이동 경로정보를 분석하는 것을 트레이스 백이라고 한다[12]. 그러므로 네트워킹 과정에 있어 안정성과 신뢰성 확보를 위하여 해당 경로들에 대한 정확한 분석이 필요하다. 본 논문에서는 기존의 연결 과정에 필요한 정보 대신 트레이스 백 정보 기반의 암호화/복호화 정보를 인증과정에 사용하고 있다. (그림 2)는 특정 송/수신자 상호간 트레이스 백의 결과를 나타내는 것이다[13-15].

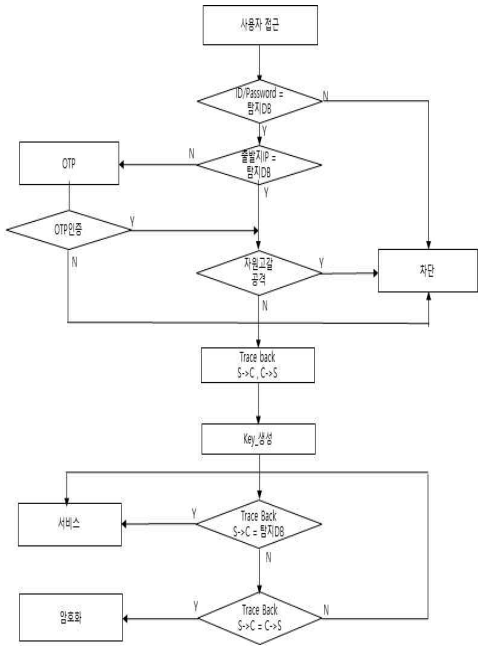
```
최대 16홉 이상의 175.114.165.254(으)로 가는 경로 추적

  1    <1 ms    <1 ms    <1 ms  10.10.0.1
  2     3 ms     2 ms     3 ms  112.220.125.185
  3     1 ms     1 ms     1 ms  10.18.156.133
  4     1 ms     2 ms     1 ms  1.213.12.205
  5     1 ms     1 ms     1 ms  1.213.12.109
  6     1 ms     2 ms     2 ms  1.208.107.221
  7     4 ms     3 ms     3 ms  203.233.45.213
  8     5 ms     6 ms     4 ms  211.44.125.117
  9     8 ms     7 ms     7 ms  10.222.15.38
 10     5 ms     4 ms     5 ms  10.222.15.135
 11     6 ms     5 ms     6 ms  10.101.0.9
 12     5 ms     5 ms     5 ms  116.126.171.122
 13    13 ms    11 ms     9 ms  1.245.26.46
 14     *        *        *     요청 시간이 만료되었습니다.
 15     *        *        *     요청 시간이 만료되었습니다.
 16     *        *        *     요청 시간이 만료되었습니다.

추적을 완료했습니다.
```

(그림 2) 트레이스 백 결과

## 3. 제안 모델 동작 과정

### 3.1 제안 모델

다음 (그림 3)은 본 논문에서 제안하는 모델의 동작 과정을 도식화 한 것을 나타낸 것이다. 본 논문에서는 사용자의 접근이 발생하면 다음 과정을 수행한다.




(그림 3) 제안모델 동작 과정

STEP 1. 사용자의 ID/Password를 탐지 DB의 내용과 비교하여 정상 사용자 여부를 분석한다.

1-1. ID/Password가 일치할 경우 STEP 2의 정상적인 출발지 정보 분석 단계를 수행하도록 한다.

1-2. ID/Password와 탐지 DB 내용이 일치 하지 않으면 차단 작업을 수행한다.

STEP 2. 출발지 IP 일치 여부를 판단한다.

2-1. 출발지 정보가 일치 하지 않을 경우, OTP 인증 과정을 수행하도록 한다.

2-2 출발지 정보가 일치하면 STEP 3의 자원고갈 공격 여부단계를 수행하도록 한다.

STEP 3. 해당 접근자의 자원고갈 공격 여부를 분석한다.

3-1. 자원고갈 공격이 발생했을 경우 해당 접근자에 대한 차단 작업을 수행한다.

3-2. 자원고갈 공격 이력이 존재하지 않을 경우 STEP.4의 상호 인증을 과정을 수행하도록 한다.

STEP 4. 서버와 클라이언트 상호 인증을 위하여 동시 트레이스 백을 수행한다.

STEP 5. 상호 인증을 위한 Key생성 작업을 수행한다.

STEP 6. 접근 클라이언트 인증을 위하여 트레이스 백

정보를 탐지 DB의 내용과 비교 분석한다.

6-1. 트레이스 백 정보가 일치하면 클라이언트의 요청 서비스를 수행한다.

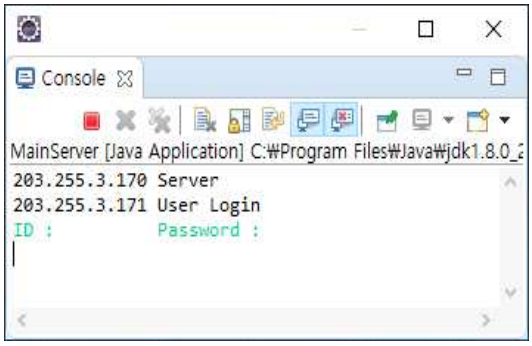
6-2. 트레이스 백 정보가 일치하지 않을 경우 연결을 바로 차단하지 않고 요청 자료를 암호화 한 후 서비스 작업을 수행한다.

STEP 7. 암호화 자료에 대한 정상적인 복호화를 클라이언트에서 수행하지 못했을 경우 해당 접근자에 대한 차단 작업을 수행하고 그 정보를 탐지 DB에 등록한다.

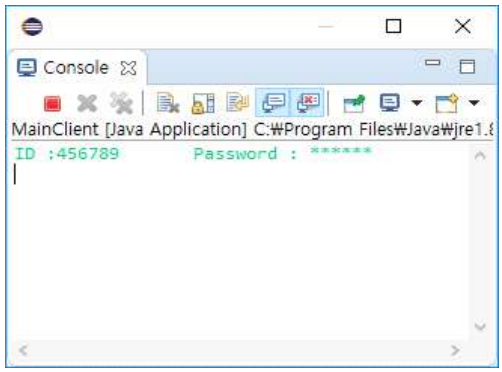
## 4. 실험 및 평가

본 논문에서 제안하는 트레이스 백 정보 기반의 서버/클라이언트 상호 인증을 위한 암호화/복호화 모델의 실험 환경은 다음과 같다. 구현을 위한 응용소프트웨어는 eclipse-workspace, java를 사용하였으며, 운영체제는 Windows 10 Education 64 비트 환경에서 실시하였다. 시스템 사양은 8GB 메모리를 채택한 i5(3Core) 3.20Ghz로 구성하였으며, 가상 네트워크 구성 후 이에 대한 실험은 와이어샤크에서 수행하였다. 아울러 실험을 위한 트레이스 백 정보 수집은 향후 시스템 클러스터링이 요구되는 국내 특정 단체 상호 연결 과정에 생성되는 라우터들의 정보를 임의로 설정하여 실험 자료로 사용하였다.

다음 (그림 4)는 출발지 주소가 203.255.3.171인 클라이언트가 서비스 요청을 시도한 목적지 주소 203.255.3.170인 서버로 접속하는 초기 과정의 정보를 나타내는 것이다.




(그림 4) 사용자 초기 접근 정보




(그림 5) 아이디/패스워드 인증 과정

위 (그림 5)는 (그림 4)의 사용자 초기정보를 기반으로 접속이 발생한 후 본 논문에서 제안하는 모델의 첫 번째 정상 사용자 인증을 위한 ID/Password를 검증하는 과정을 나타내는 것이다.

(그림 6)은 클라이언트의 ID/Password 정보를 서버에서 정상적으로 인증한 결과를 보이고 있다.

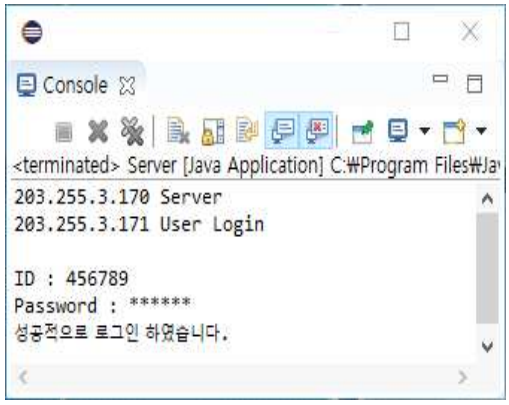
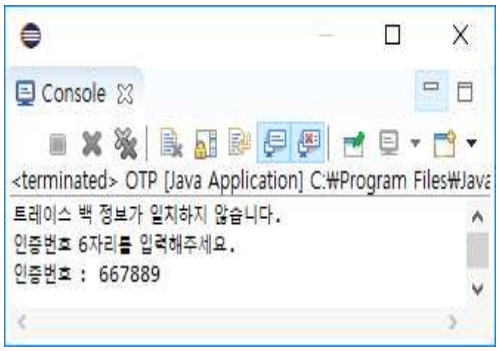


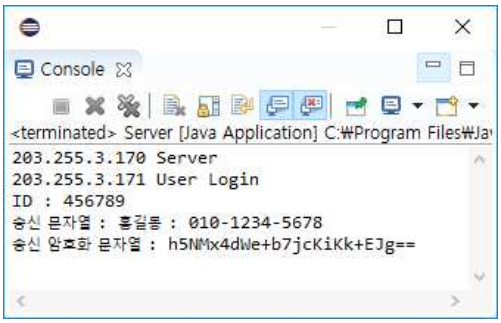

그림 6. 정상적인 사용자 로그인

(그림 7)은 ID/Password 인증 과정을 정상적으로 수행한 후, IP 스푸핑 공격자 여부를 확인하기 위한 과정이다. 이 과정에서는 정상적인 트레이스 백 정보를 비교하고, 불일치할 경우 OTP 인증에 대한 그 수행 과정을 보이고 있다.



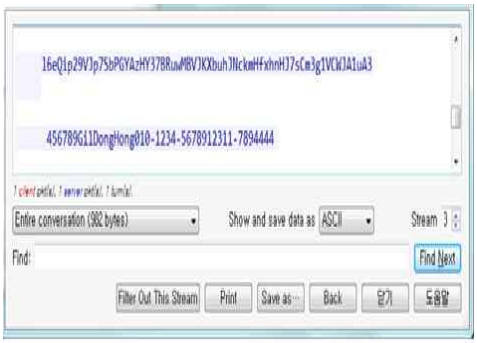

(그림 7) 원타임 패스워드 인증 과정

(그림 8)은 클라이언트와 서버에서 동시 트레이스 백을 수행한 후 해당 정보에서 상호 약속한 특정 IP 정보를 이용하여 서비스 정보를 암호화 시킨 다음 이를 클라이언트로 전송한 결과를 나타내는 것이다.

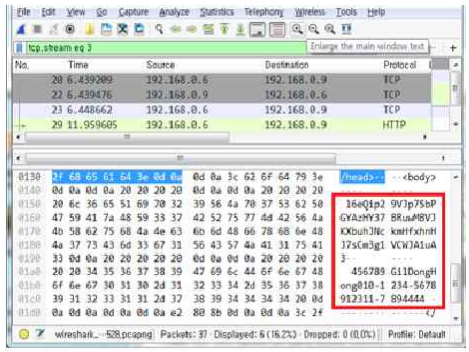



(그림 8) 사용자 인증을 위한 암호화 과정

(그림 9)와 (그림 10)은 (그림 8)의 수행 과정을 와이어샤크에서 가상 네트워크로 구성하여 암호화 시킨 메시지를 클라이언트로 전송하는 과정을 보이는 것이다.




(그림 9) 서버에서 암호화 과정을 수행한 서비스 자료



(그림 10) 클라이언트로 전송중인 서비스 자료

(그림 11)은 정상적인 사용자 접근일 경우 (그림 8)의 암호문 서비스를 정상적으로 복호화 시킨 결과를 보이는 것이다. 즉, 서버에서 클라이언트로 암호화 시킨 서비스 문자열을 클라이언트에서 받은 복호화 시킨 결과를 보이는 것이다. 이 과정에서 정상적인 복호화 과정을 수행하지 못 할 경우 본 논문에서는 차단 작업을 수행하게 된다.

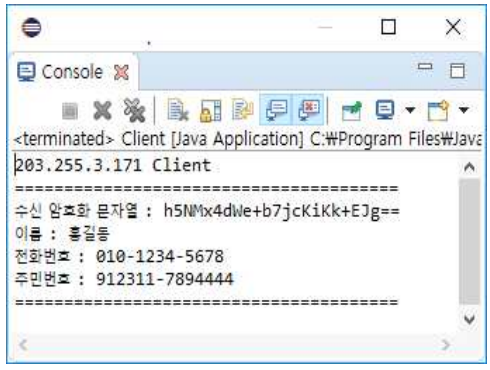



그림 11. 사용자 인증을 위한 복호화 과정

(그림 12)는 정상적인 복호화 과정을 수행하지 못한 클라이언트에 대하여 차단 작업을 수행한 결과를 나타내는 것이다.

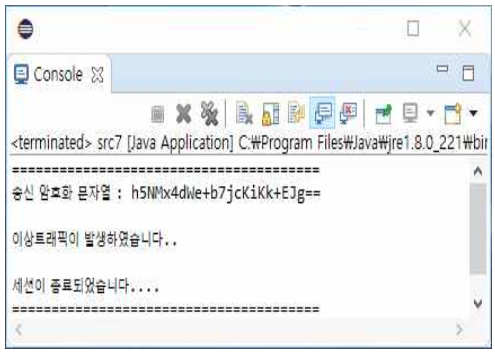



그림 12. 사용자 인증을 위한 복호화 과정

## 5. 결 론

발전중인 4차 산업 혁명의 융합 과정에는 서비스 안정성과 투명성을 보장하기 위해 정보통신 기술이 반드시 필요하다. 그렇지만 이러한 통신기술의 발전은 네트워크 구성의 다양성으로 인하여 불법적인 공격자들의 집중적인 표적이 되고 있다.

본 논문은 클라우드 서비스를 수행하는 특정 서버를 대상으로 IP 스푸핑 공격이 발생할 경우 이를 탐지하기 위한 모델을 제시한 것이다. 본 논문의 탐지 모델은 정상적인 사용자 인증 과정에 기존의 OTP 인증 및 트레이스 백 정보 기반의 암호화/복호화 과정을 추가하여 사용하고 있다. 이는 OTP 인증 기법에서 발생하는 빈번한 OTP 사용을 감소시키고 서비스 가용성을 향상시킬 수 있기 때문이다. 즉, 불법적인 접근을 시도하는 공격자의 경우 본 논문에서 제안하는 정상적인 암호화/복호화 과정을 수행할 수 없기 때문에 최종 접근에 실패하게 되는 것이다. 아울러 IP 스푸핑 공격 과정에서 발생하는 자원고갈 공격 정보를 탐지한 후 클라우드를 구성하는 관련 서버에서도 해당 공격 정보를 공유하여 신속한 대응이 가능하도록 설계하였다. 향후 연구 과제로는 IP 스푸핑 공격이 동시에 다수의 공격자로부터 발생할 경우 이들 공격 정보를 신속하게 공유한 후 정확한 대응을 할 수 있는 시스템 연구가 진행되어야 할 것이다.

## 참고문헌

[1] Zargar, S.T.,Joshi, J.and Tipper, D. 2013. A surver of defense mechanisms against distributed denial of service DDoS flooding attacks, Communications Survers & Tutorials, IEEE, 15(4) : 2046-2069

[2] 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.

[3] 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.

[4] Y, H. Jung, "A Study of the Android OS based touch macro detection method", Korea Univ., 2016.

[5] Telecommunication Technology Association 2008. Botnat trend and respond technology present, TTA Journal, 118 (Special Report) : 58-65.

[6] W. I. Kim, S. H. Yoo, Y. C. Jang and C.H. Lee, "A Design and Implementation of Abnormal Permission-Flow Detecting Security Module", J. of Korean Institute of Next Generation Computin-g, Vol.10, No. 2, pp 66-74, 2014.

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

[8] D. Pansa and T. Chomsiri, Architecture and Protocols for Secure LAN by Using a Software-level Certificate and

Cancellation of ARP Protocol, Third 2008 International Conference on Convergence and Hybrid Information Technology, pp. 21~26, 2008.

[9] Shin, Y. H. Lim, G. H and Im, E. G. 2009. A Research on the possibility of ARP spoofing attack in SCADA System Based on TCP/IP environment. Convergence security journal, 9(3) : 9-17.

[10] D.-S. Choi, D.-H. Oh, J.-S. Park, J.-C. Ha, An Improved Round Reduction Attack on Triple DES Using Fault Inj-ection in Loop Statement, Journal of The Korea Institute of Information Security & Crypto logy, Vol. 22, No. 4. pp 709~717, 2012.

[11] M-H Kim, H-C Beak, S-W Hong and J-H Park, 2015. An Encrypted Service Data Model for Using Illegal Applications of the Government Civil Affairs Service under Big Data Environments, Converg-ence security journal, Vol. 15No. 7, pp. 31-38, 2015.

[12] C. H, An, H. C. Baek, Y. G. Seo, W. C. Jeong, and S. B. Kim. "Designing Mutual Cooperation Security Model for IP Spoofing Attacks about Medical Cluster Basis Big Data Environment", Convergence security journal, Vol. 16, No. 7, pp. 21-29, 2016.

[13] Y-J Baek, S-W Hong, J-H Park, G-W Gang, S-B Kim, "A Macro Attacks Detection Model Based on Trace Back Information", Convergence security journal, Vol. 18, No. 5, pp. 113-120, 2018.

[14] 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, 2015.

[15] C. H. An, "Medical treatment cluster composition and security model design of regional public hospitals in Korea for telemedicine", Gyengsang Univ., 2016.

## 〔저자소개〕

백 용 진(Yong-Jin Baek)
2015년 2월 경남과학기술대학교 컴퓨터공학과 학사
2019년 2월 경상대학교 대학원 컴퓨터과학과 석사 졸업
2019년 현재 경상대학교 대학원 컴퓨터과학과 박사 과정

email : qhanffkwk@nate.com

홍 석 원 (Suk-Won Hong)
2003년 2월 경남과학기술대학교 컴퓨터공학과 학사
2006년 2월 경상대학교 컴퓨터과학과 석사
2011년 2월 경상대학교 컴퓨터과학과 박사
1999년 4월 ~ 현재 : 경남도립 거창대학

email : swhong@gc.ac.kr

김 상 복 (Sang-Bok Kim)
1979년 2월 중앙대학교 전자공학과 학사
1981년 2월 중앙대학교 전자공학과 석사
1989년 2월 중앙대학교 전자공학과 박사
1984년 3월 ~ 현재 : 경상대학교 교수

email : sbkim@gnu.ac.kr