Journal of Knowledge Information Technology and Systems(JKITS), Vol. 14, No. 6, pp. 683~691, December 2019
https://doi.org/10.34163/jkits.2019.14.6.011

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Asymmetric Key Cryptographic Authentication Model for IP Spoofing in Cloud Environments

Young Jin Baek[1], Suk-Won Hong[2], Chang-Hee Lee[3], Sang-Bok Kim*[1]

[1]*Department of Computer Science, Gyeongsang National University*
[2]*Gyeongnam Provincial Geochang College Information Support Center*
[3]*Division of Health Administration, Jinju Health College*

ABSTRACT

Today's cloud-based network services demand strong security. However, in an environment where real-time provision of service resources is essential, it is caused by an enhanced security policy, which causes a decrease in quality of service availability. In addition, IP spoofing attacks, which can severely damage network availability and integrity, can be more frequent in cloud service environments. Therefore, systems that perform cloud services need to establish new security policies and systems that can guarantee availability and integrity. Conventional detection and response methods for IP spoofing include analyzing traceback information and performing authentication through OTP when different paths occur. However, this method can degrade service availability because OTP is generated every time a different path is detected. In addition, in order to improve this, a pattern-based encryption scheme may leak decryption information by a sniffing attack. In order to improve this problem, this paper replaces the authentication process with the normal decryption based on traceback information instead of the encryption process after analyzing the existing access information. Based on this, reauthentication over OTP is performed only when the client's IP is different and when normal decryption cannot be performed. In addition, it solved the problem of excessive OTP generation and presented an authentication model that enables continuous service in real time.

KEYWORDS: Traceback, Cloud computing, IP spoofing, Encryption, Asymmetric key

ARTICLE INFO: Received 9 November 2019, Revised 7 December 2019, Accepted 7 December 2019.

*Corresponding author is with the Department of Computer Science, Gyeongsang National University, 501, Jinju-daero, Jinju-si, Gyeongsangnam-do, 52828, KOREA.
E-mail address: sbkim@gnu.ac.kr

1. 서 론

오늘날 네트워크 기반의 공격 형태는 클라우드 서비스를 수행하고 있는 시스템으로 집중되고 있다. 네트워크 기반의 다양한 공격 중 IP 스푸핑 공격(IP Spoofing Attacks)은 상호 신뢰하고 있는 클라이언트와 서버의 IP 주소를 이용하여 불법적인 접근을 시도하는 공격 형태이다[1].

보안 시스템이 강력하게 구축되어 있는 서버에 대한 공격자들의 직접적인 공격 빈도수는 그렇지 못한 클라이언트 환경에서 보다 상대적으로 적게 나타난다. 그렇지만 IP 스푸핑 공격을 시도하는 공격자들은 서버에서 신뢰하고 있는 클라이언트의 IP 정보를 이용하여 목표로 하는 서버를 공격하게 된다. 그러므로 이러한 IP 스푸핑 공격은 상호 신뢰 관계를 유지하는 시스템 상호간 IP기반의 인증 과정을 수행하기 때문에 클라우드 서비스 환경에서는 그 공격 빈도수가 더욱 증가할 수 있다.

IP 스푸핑 공격에 대한 기존의 탐지와 대응 방식에는 접근을 요청한 클라이언트의 트레이스 백 정보를 분석한 후 접속 여부를 결정하는 방식이 있다[2,3].

하지만 접근을 요청한 클라이언트에 대한 단순한 트레이스 백 정보의 분석 방식은 경유 라우터들의 IP 정보를 모두 비교하기 때문에 빈번한 False Positive오류를 발생시킬 수 있다. 아울러 이로 인한 OTP(One Time Password)를 지속적으로 요청하기 때문에 서비스 가용성에 대한 문제점을 노출시키고 있다.

본 논문은 클라우드 서비스를 수행하는 환경에서 IP 스푸핑 공격 발생시 이에 대한 탐지 및 대응, 그리고 서비스 가용성을 보장하기 위한 것이다. 아울러 분석 및 인증 과정에서 빈번하게 발생하는 OTP 인증 방식 대신 암호화 및 복호화 과정을 먼저 수행하도록 하여 기존의 인증 과정을 대체하도록 하였다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 관련 연구를 살펴보고, 3장에서 트레이스 백 정보를 이용한 비대칭키 기반의 암호화 인증 모델의 처리 과정을 나타내었다. 그 다음 4장에서는 제안 모델의 전반적인 동작 과정에 대한 결과를 실험을 통해 보이고 있다. 마지막 결론에서는 본 논문의 향후 응용 분야에 대한 언급을 하였다.

2. 관련연구

2.1 클라우드 서비스

클라우드 서비스란 네트워킹을 기반으로 인프라, 플랫폼, 어플리케이션 등에 대한 서비스를 실시하고 이에 대한 요금을 부가하는 환경을 의미한다[4,5]. 기존의 일반적인 서버/클라이언트 환경에서는 하나의 서버를 기반으로 다수의 클라이언트에 대한 서비스가 이루어지고 있다. 반면에 클라우드 서비스 환경에서는 다양한 특정 서비스를 다수의 클라이언트에게 서비스 작업을 수행한다. 이에 따라 실시간 서비스를 요구하는 클라우드 서비스는 그 안정성과 가용성을 위하여 기존의 일반적인 네트워크 환경의 보안정책 보다 더욱 강화된 보안 시스템 운영이 필요하며, 전반적인 서비스 과정에 대한 새로운 보안 모델 구축이 필요하다.

2.2 IP 스푸핑

네트워크 기반의 다양한 공격 기법 중 IP 스푸핑은 전문 해커들이 주로 사용하는 공격 기법으로 그 공격 특성상 침해를 당한 사이트에 엄청난 피해를 준다[6].

클라우드 상에 존재하는 서버와 클라이언트의 연결 과정에는 상호 신뢰하는 IP 주소기반의 인증

기법을 사용한다. IP 스푸핑은 이러한 인증 과정에 필요한 특정 신뢰시스템의 IP를 획득한 후 이를 이용하여 불법적인 접근을 시도한다[7].

<그림 1>은 공격자가 IP 스푸핑을 시도하는 과정을 나타내는 것으로, 신뢰호스트와 타겟 서버 간 연결 차단 표시는 네트워크상에는 둘 이상의 IP가 존재할 수 없기 때문에 공격자에 의해 신뢰호스트가 다운되는 과정을 보여 주는 것이다. 즉, 공격자는 IP를 획득한 신뢰호스트에 자원 고갈 공격을 시도하여 해당 시스템이 정상적인 서비스 수행을 할 수 없도록 만드는 것이다.

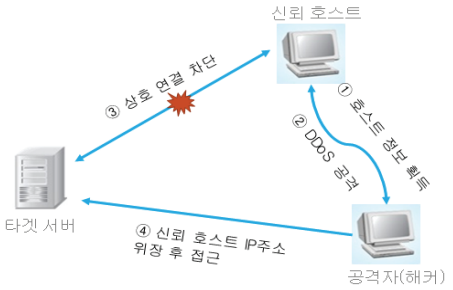

그림 1. IP 스푸핑
Figure 1. IP spoofing

2.3 트레이스 백

원거리 송신자와 수신자 사이에는 네트워크 경로 관리를 위한 라우터들이 존재한다. 트레이스 백이란 송신자와 수신자 사이에 존재하는 라우터들의 IP 정보를 기반으로 경로 정보를 분석하고 제공해 주는 프로그램이다. 본 논문에서는 이러한 트레이스 백 정보를 기반으로 공격 탐지 과정에 기존 논문의 트레이스 백 정보의 순차적인 단순 비교 방식과 임계치 비교 방식을 상호 비교하여 서비스 가용성에 대한 평가를 하였다[8-10].

2.4 암호화

암호화란 송신자와 수신자 상호 간 정보 교환에 있어 해당 정보의 내용을 인가받지 않은 사용자가 볼 수 없도록 변환시키는 과정이라고 할 수 있다.

본 논문에서는 스니핑 공격 발생시 암호화/복호화 키의 안전성 문제 해결과 클라이언트에 대한 인증 정보로 활용하기 위해 트레이스 백 정보를 활용하여 <그림 2>와 같이 비대칭키 방식의 암호화 알고리즘을 사용하였다[11-13].

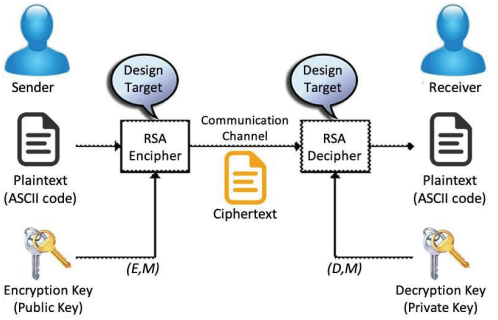

그림 2. 비대칭키 암호화
Figure 2. Asymmetric key encryption

3. 제안 모델 동작과정

본 논문에서 제안하는 클라우드 서비스 모델은 향후 33개 전국지방의료원과 협력/협진 의료기관의 의료정보를 전국지방의료원연합회에서 클러스터화 시킨 후 이를 관련기관 및 협력/협진 의료기관으로 클라우드 서비스 하는 과정을 <그림 3>과 같이 나타내었다.

본 논문의 클라우드 서비스 환경은 전국지방의료원연합회와 각 서비스 대상 협력/협진 기관 상호 인증에 필요한 공개키 수집을 위하여 상호 트레이스 백을 수행하였다. 그 다음 이 과정에서 생성된 경유 라우터들의 IP와 홉을 기반으로 상호 약속에 의한 공개키를 생성한다.

이렇게 생성한 공개키를 이용하여 서버에서는

인증에 필요한 암호문을 생성하고 해당 서비스를 요청한 클라이언트로 전송하여 인증 과정을 수행하도록 한다.

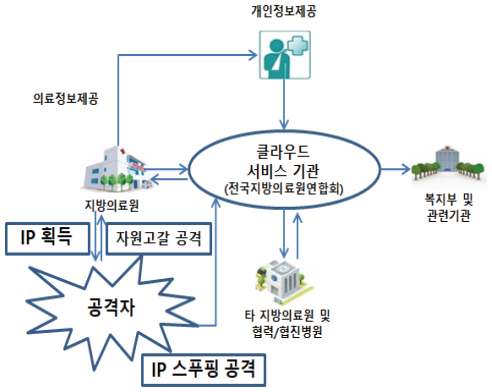

그림 3. 제안모델의 클라우드 서비스 환경
Figure 3. Cloud service environment of proposed model

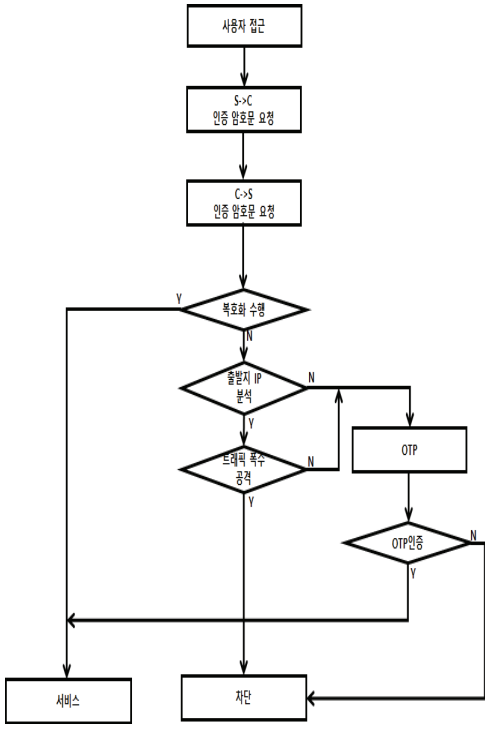

그림 4. 제안모델 동작과정
Figure 4. Proposed model operation processing

본 논문에서는 전국지방의료원과 협력/협진 의료기관 상호 발생하는 의료정보를 클러스터화 시키고 이를 전국지방의료원연합회에 구축하는 것을 가정하였다. 그리고 이를 클라우드로 서비스하는 과정에서 요구되는 사용자 인증 및 서비스 수행 과정을 <그림 4>를 통하여 나타내었다.

STEP 1. 클라이언트(C)의 서비스 요청 발생.

STEP 2. 인증을 위한 암호문 생성 후 서버(S)에서 클라이언트(C)로 인증을 위한 암호문 전송.

STEP 3. 암호문을 수신한 클라이언트는 해당 암호문을 복호화 시킨 후 결과를 서버로 전송.

STEP 4. 복호화 정보를 수신한 서버는 클라이언트에 대한 인증 과정 수행.

4-1. 클라이언트가 복호화 과정을 정상적으로 수행했으면 클라이언트에 대한 서비스를 실시한다.

4-2. 클라이언트가 정상적인 복호화 과정을 수행하지 못했다면 정상적인 예외 IP 검증을 위해 STEP 5. 과정을 수행한다.

STEP 5. 서비스를 요청한 클라이언트의 IP를 분석한 후 그 결과에 따라 STEP 6., STEP 7. 과정을 각각 수행한다.

5-1. 서비스 요청 클라이언트의 IP 주소가 일치할 경우 트래픽 폭주 공격 이력을 분석하기 위해 STEP 6. 과정을 수행한다.

5-2. 서비스 요청 클라이언트의 IP 주소가 일치하지 않는 경우 정상적인 예외 IP 분석을 위해 STEP 7. 과정을 수행한다.

STEP 6. 해당 IP의 트래픽 폭주 공격 여부를 분석한다.

6-1. 트래픽 폭주 발생 이력이 없는 클라이언트일 경우 정상적인 예외 IP로 가정하고 STEP 7. 과정을 수행한다.

6-2. 트래픽 폭주 발생 이력이 있는 클라이

언트의 IP일 경우 차단 작업을 수행한다.

STEP 7. 정상적인 예외 IP 검증을 위해 서비스를 요청한 클라이언트로 OTP를 전송한다.

STEP 8. OTP 처리 결과를 분석한 후 서비스 또는 차단 작업을 수행한다.

4. 실험 및 평가

본 논문에서 제안하는 트레이스 백 정보 기반의 서버/클라이언트 상호 인증을 위한 비대칭키 기반 암호화/복호화 과정에 대한 실험 환경은 다음과 같다. 먼저 구현을 위한 응용소프트웨어는 eclipse-workspace, j ava를 사용하였으며, 운영체제는 Windows 10 Education 64비트 환경에서 채택하였다. 시스템 사양은 8GB 메모리를 채택한 i5(3cor e) 3.20Ghz로 사용하였다.

4.1 트레이스 백 정보 획득

```
최대 16홉 이상의
static.221-132-73-150.nexg.net [221.132.73.150](으)로 가는 경로 추적:

  1    1 ms    1 ms    1 ms  10.11.20.249
  2   <1 ms   <1 ms   <1 ms  10.11.100.254
  3   12 ms    3 ms    3 ms  175.114.165.225
  4    4 ms   <1 ms   <1 ms  1.245.26.45
  5   <1 ms   <1 ms   <1 ms  116.126.171.121
  6    1 ms    1 ms    2 ms  10.101.0.8
  7   10 ms    7 ms    7 ms  10.222.10.144
  8    8 ms    6 ms    7 ms  58.229.12.214
  9   11 ms    8 ms    7 ms  128.134.10.85
 10    4 ms    9 ms    5 ms  128.134.10.178
 11   19 ms   19 ms    8 ms  203.246.169.133
 12    4 ms    9 ms    5 ms  203.246.170.242
 13   13 ms   14 ms    6 ms  static.122-199-254-160.nexg.net [122.199.254.160]
 14    8 ms    *       7 ms  172.22.30.65
 15    7 ms    9 ms    7 ms  static.221-132-73-150.nexg.net [221.132.73.150]

추적을 완료했습니다.
```

그림 5. 트레이스 백 정보
Figure 5. Traceback information

본 논문에서 요구되는 트레이스 백 정보는 향후 의료정보 클러스터링이 요구되는 특정 지방의료원의 네트워킹 과정에서 발생하는 경유 라우터들의 정보를 관계자들의 협조를 통해 <그림 5>와 같이 그 예를 보였다[14].

4.2 암호화 복호화 과정

<그림 6>은 클라우드 서비스를 요청한 클라이언트에 대한 인증 과정을 위해 클라이언트의 트레이스 백 정보의 일부(203.255.3.2 1)를 공개키로 암호화 시킨 결과를 보이고 있다. 본 논문에서는 서버에서 생성시킨 암호문을 클라이언트로 전송하여 이에 대한 복호화 여부로 인증 과정을 수행하기 때문에 정상적인 사용자에 대한 단절과 과도한 OTP 발생을 개선시켰다.

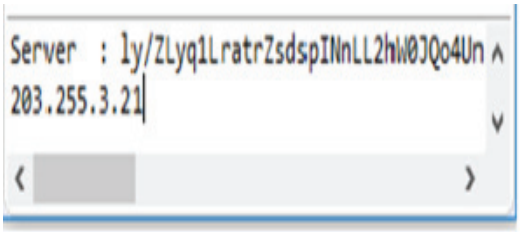

그림 6. 클라이언트 인증을 위한 암호문
Figure 6. Ciphertext for client authentication

<그림 7>은 서비스를 요청한 클라이언트에 대해 서버에서 인증을 위해 전송한 암호문을 클라이언트에서 정상적으로 수신한 결과를 나타낸 것이다.

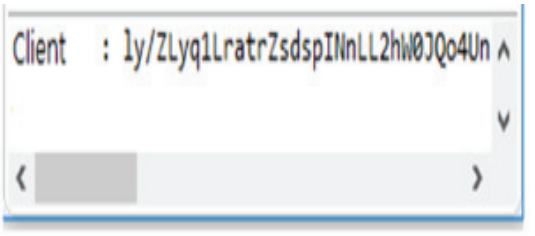

그림 7. 클라이언트에서 수신한 암호문
Figure 7. Ciphertext received by client

<그림 8>은 서비스를 요청한 클라이언트에서 서버로부터 수신한 암호문을 복호화시키는 과정과 그 결과를 보이는 것이다.

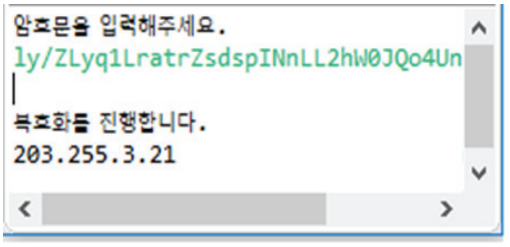

그림 8. 클라이언트에서 암호문 복호화 과정
Figure 8. Decryption process on the client

4.3 신규 경로 클라이언트 인증 과정

<그림 9>는 새로운 클라우드 서비스 가입자이거나 정상적인 경로를 벗어나 서비스를 요청한 클라이언트에 대한 신규 인증을 위해 OTP를 발생시켜 인증 과정을 수행하는 것을 보이고 있다. 본 논문에서는 또한 이 과정을 통해 서버에서 신뢰를 하고 있는 클라이언트의 IP를 도용하여 IP 스푸핑을 시도하는 공격을 탐지하기 위해서도 사용하고 있다.

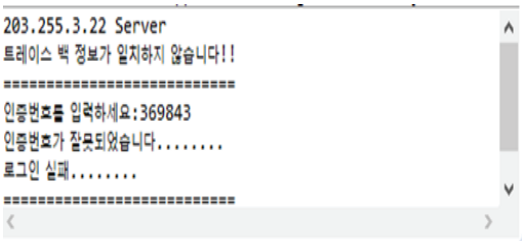

그림 9. 신규 경로 클라이언트 인증 과정
Figure 9. Authentication process for new path client

4.4 평가

<표 1>은 클라우드 서비스 환경에서 서비스 가용성과 관련하여 OTP 발생 횟수를 기존 방식과 비교를 통해 그 효율성을 나타낸 것이다. <표 1>의 기존방식 1은 트레이스 백 정보를 순차적으로 상호 비교하는 방식을 의미한다. 기존방식 1은 ID/Password, 트레이스 백 정보를 단순 비교하기 때문에 해당 정보가 불일치하는 경우 매번 OTP를 발생시킨다. 기존방식 2는 기존방식 1의 문제점을 개선하기 위해 유클리안 거리 좌표를 기반으로 인증에 필요한 임계 범위를 설정하여 OTP 발생을 감소시키고 있다. 그렇지만 이 경우에도 지속적인 OTP가 발생하고 있다. <표 1>의 결과를 통해 각 단계별 인증 과정에서 제안 모델은 OTP 인증 과정이 거의 발생하지 않음을 알 수 있다. 특히 클라우드 서비스 과정에 존재하는 홉의 수가 증가할수록 OTP 인증으로 인한 서비스 단절 문제를 제안 모델에서는 안정적으로 유지할 수 있다는 것을 알 수 있다.

표 1. OTP 발생 횟수에 따른 서비스 가용성 비교
Table 1. Service availability comparison by OTP count

비교방식 / OTP발생	기존방식 1 (트레이스 백 단순 비교)	기존방식 2 (임계치 기반 비교)	제안모델 (비대칭키 인증)
초기 인증 과정	ID, Password비교 불일치:OTP(1회)	ID, Password비교 불일치:OTP(1회)	암호문 인증 OTP(0회)
출발지 인증 과정	출발지 IP 비교 불일치:OTP(1회)	출발지 IP 비교 불일치:OTP(1회)	출발지 IP 비교 불일치:OTP(1회)
홉(N)별 인증 과정	최소 OTP(0회) 최대 OTP(N회)	최소 OTP(0회) 최대 OTP (N-임계치 일치 회수)	출발지 IP 비교 불일치:OTP(1회)

5. 결 론

본 논문은 향후 원격진료 과정에서 요구되는 전국지방의료원들의 의료정보 클러스터링 구축과 클라우드 서비스에 대비하여 서버와 클라이언트 상

호 접근성 및 가용성을 향상시키기 위해 비대칭키 기반의 암호화 인증 모델을 제시한 것이다.

클라우드 환경하에서의 서비스 제공 과정에 대한 신뢰도 문제는 클라이언트에게 해당 서비스의 재사용 여부를 결정하는 중요 요인으로 작용한다. 그러므로 안정된 접속 보장이 가능한 능동적이고 강화된 인증 과정이 요구된다.

클라우드 서비스 환경에서 클라이언트의 서비스 요청 발생시 기존의 일반적인 인증 방식은 상호 트레이스 백 정보를 생성시킨 후 이에 대한 단순 비교 방식을 기반으로 한다. 그렇지만 인증을 위한 단순 비교 방식은 정상적인 클라이언트의 접속을 비정상적인 접속으로 판정하여 해당 접속을 차단하는 경우가 발생할 수 있다. 아울러 경유하는 모든 라우터에 대해 IP 정보를 순차적으로 비교하기 때문에 과도한 OTP를 발생시킬 수 있다.

본 논문은 이러한 OTP 발생 문제와 탐지 오류를 개선하기 위해 비대칭키 암호화 기법을 이용하였다. 특히 스니핑 공격에 취약한 로그인 아이디, 패스워드 검증 방식이 아닌 비대칭키 암호화 기법을 기반으로 인증 과정을 강화했으며, 연결성에 대한 가용성도 확보하였다. 향후 연구 과제로는 클라우드 환경하에서 더욱 강화된 보안 협력 체계를 구축할 수 있는 네트워크 기반의 클러스터링 보안시스템 구축에 대한 연구가 함께 진행되어야 할 것이다.

References

[1] Zargar, S.T.,Joshi, J.and Tipper, D. 2013. *A surver of defense mechanisms against distributed denial of service (DDoS) flooding attacks*, Communications Surveys & 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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] C-H. Ahn, H-C. Baek, Y-G Seo, W-C

Jeong, and J-Y. Park, *Design mutual cooperation security model for IP spoofing attack about medical cluster basis big Data environment,* Journal of the Korea Convergence Security Associate, Vol. 16, No. 7, pp. 21-29, 2016.

[9] Y. Liu, H-C. Baek, J-Y. Park, and S-B. Kim, *Model design for reduce OTP reauthorization based on euclidean distance,* Journal of the Korea Institute of Information and Communication Engineering, Vol. 12, No. 5, pp. 737-745, 2017.

[10] Y. Liu, H-C. Baek, J-Y. Park, and S-B. Kim, *An improved model design for traceback analysis time Based on euclidean distance to IP spoofing attack*, Korea Convergence Security Association, Vol. 17, No. 5, Dec. 2017.

[11] W-L. Choi, K-W. Shin, *2,048 bits RSA public-key cryptography processor based on 32-bit Montgomery modular multiplier,* J. Korea Inst. Inf. Commun. Eng, Vol. 21, No. 8, pp. 1471-1479, 2017.

[12] A. Kauther, S. Sami, and A. Ahmed, *Enhancement of hardware modular multiplier radix-4 algorithm for fast RSA cryptosystem*, International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), Khartoum, Sudan, pp. 692-696, 2013.

[13] S. Rohith, and C. Mahesh, *FPGA implementation of 16 bit RSA cryptosystem for text message*, International Journal of Computer Applications, Vol. 92, No. 8, 2014.

클라우드 환경에서 IP 스푸핑 대응을 위한 비대칭키 암호화 인증 모델

백용진[1], 홍석원[2], 이창희[3], 김상복[4]

[1] *경상대학교 컴퓨터과학과 박사과정*
[2] *경남도립거창대학 정보지원센터 팀장*
[3] *진주보건대학교 보건행정과 교수*
[4] *경상대학교 컴퓨터과학과 교수*

요 약

오늘날 클라우드 기반의 네트워크 서비스 는 강화된 보안 시스템 구축을 요구하고 있다. 그렇지만 서비스 자원의 실시간 제공이 필수적인 환경에서는 강화된 보안 정책이 서비스 가용성에 대한 질 저하의 원인으로 나타나고 있다. 아울러 네트워크 서비스 가용성 및 무결성에 치명적인 손상을 가져 오는 IP 스푸핑 공격은 클라우드 서비스 환경에서 그 공격 빈도수가 더욱 증가할 수 있다. 그러므로 클라우드 서비스를 수행하는 시스템들은 서비스 가용성 및 무결성 보장이 가능한 새로운 보안 정책과 시스템 구축이 필요하다. IP 스푸핑에 대한 기존의 탐지와 대응 방식에는 트레이스 백 정보를 분석한 후 상이한 경로 탐지 시 OTP를 통한 인증 과정을 수행하는 방식이 있다. 그러나 이러한 방식은 상이한 경로가 탐지 될 때 마다 매번 OTP를 발생시키기 때문에 서비스 가용성을 저하 시킬 수 있다. 또한 이를 개선하기 위한 일정 패턴 기반의 암호화 방식은 스니핑 공격에 의해 복호화 정보가 유출될 수 있다. 본 논문은 이러한 문제점을 개선하기 위해 기존의 접근 정보 분석 후 암호화 과정을 수행하지 않고 트레이스 백 정보 기반의 정상적인 복호화 수행 여부로 인증 과정을 대신하도록 하였다. 이를 통해 출발지 IP가 상이한 경우와 정상적인 복호화를 수행할 수 없는 경우에만 OTP를 통한 재인증 과정을 수행하도록 하였다. 아울러 기존의 과도한 OTP 발생에 대한 문제점을 해결하고 지속적인 서비스가 실시간 가능한 인증 모델을 제시하였다.

Young Jin Baek received the Master´s degree in the Department of Computer Science from Gyeongsang National University in 2018. His current research interests include network architecture, bigdata security, network security.
E-mail address: a2633558a@naver.com

Suk Won Hong received the Ph.D. degree in the Department of Computer Science from Gyeongsang National University in 2011. His current research interests include network, multimedia.

E-mail address: swhong@gc.ac.kr

Chang Hee Lee received the Ph.D. He is a professor of health administration at Jinju Health College. His current research interests include Software Engineering.
E-mail address: chlee1881@hanmail.net

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