Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Model Design for Reduce OTP Reauthorization Based on Euclidean Distance

Yang Liu[1], Hyun Chul Baek[2], Jae-Heung Park[1], Sang-Bok Kim[*1]

[1]*Department of Computer Science, Gyeongsang National University*

[2]*Department of Smart Information Convergence, Gyeongnam Provincial Namhae College*

ABSTRACT

Nowadays, intelligence communications technology is developing rapidly in a cloud computing environment with big data services. With the change of the network environment, the protection function for increasing information exchange process on the Internet and important intelligence materials needs to be further developed. Intelligence protection based on the internet has OTP authentication and encryption technology for network for the detection technology with non-normal general access. But the weaknesses of these technologies are being discovered in a variety of attack technologies. In particular, attackers with high-end illegal access technologies frequently try IP spoofing attacks. That is, it uses the cloud hosting intelligence that can build mutual trust to constantly try increase the trust relationship in the cloud service environment by illegal attacks. In order to improve the accessibility of information service in the cloud computing environment, this study analyzes the traceback information by using the Euclidean distance law in mathematics. In this study, the IP value of each hop is dually grouped, and the Euclidean distance is calculated by the two sets of coordinates. The chart changes composed of these datas are then calculated. Then the study will analyze and change the appropriate information for OTP authentication or encryption, and then obtain information to reduce the implementation process of OTP authentication.

KEYWORDS: Cloud Computing, Euclidean distance, OTP, Traceback

ARTICLE INFO: Received 13 September 2017, Revised 2 October 2017, Accepted 13 October 2017.

[*]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 정보 통신 기술의 발달은 인터넷뱅킹, 문서 발급, 증권 거래, 인터넷 쇼핑 등의 다양한 서비스들을 온라인으로 제공하고 있다. 이에 따라 온라인상으로 이루어지는 정보의 상호 교환 과정에 중요 정보 자료에 대한 보호 기능이 한층 요구되는 상황이다[1-2].

정보 보호에 사용되는 기법에는 일반적으로 불법적인 접근에 대한 탐지 기법과 OT P를 이용한 인증 기법, 암호화 기법이 사용되고 있다[3-5]. 그렇지만 이러한 기법들은 빠르게 발전하고 있는 다양한 공격에 취약점을 보이고 있다. 또한 클라우드 컴퓨팅 기반의 빅 데이터 환경은 공격자들의 집중적인 공격 대상이 될 수 있다. 특히 고도의 불법적인 접근 기술을 보유하고 있는 공격자들은 주로 IP 스푸핑 공격을 시도한다. 해당 공격 기법은 상호 신뢰 관계에 있는 클라우드 호스트 정보를 이용하여 불법적인 공격을 시도하기 때문에 클라우드 서비스 환경에서는 이러한 신뢰 관계를 이용한 공격 빈도가 더욱 증가할 수 있다[6-7].

IP 스푸핑 공격에 대한 기존 탐지 방식에는 트레이스 백 정보를 비교하여 정상적인 접근 여부를 판정하는 방식이 사용되고 있다. 그렇지만 단순 트레이스 백 정보의 비교는 정상적인 사용자를 공격으로 판정하는 오류가 발생할 수 있다. 그러므로 이와 같은 경우에 대비하여 OTP를 이용한 재인증 과정을 수행하게 된다. 하지만 이러한 트레이스 백 정보 비교 후 재인증을 위한 OTP 전송 방식은 경유하는 홉의 IP 변동이 발생할 때 마다 이에 대한 오버헤드를 초래할 수 있다[8-10].

본 논문은 클라우드 환경에서 접근성을 향상시키기 위하여 기존의 트레이스 백 정보의 분석 과정에 수학적 유클리드 거리 계산식을 이용하였다.

본 논문의 유클리드 거리 좌표는 각 홉이 보유하고 있는 IP 값을 각 두 개씩 짝을 지어 거리 좌표로 사용하였다. 그 다음 이들 좌표 값을 그래프로 나타낸 후 이에 대한 변이 추적을 하였다. 아울러 해당 변이 정보의 분석 후 OTP 전송이나 암호화 과정을 수행 하도록 했기 때문에 재인증 과정에서 요구되는 OTP 전송의 오버헤드를 감소시킬 수 있도록 하였다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 관련 연구를 살펴보고, 3장에서는 트레이스 백 정보를 이용한 유클리드 거리 좌표 생성 후 IP 변이에 대한 분석과정을 수행할 수 있는 모델을 설계하였다. 그 다음 4장에서는 유클리드 거리 계산을 통하여 도출한 좌표를 이용하여 유클리드 거리 값 분포도와 임계치를 설정하여 정상적인 사용자 여부를 분석한 후 OTP 전송과 암호화 과정을 각각 수행하도록 하였다. 마지막 결론 부분은 본 논문의 향후 이용 가능성에 대한 언급을 하였다.

2. 관련연구

스푸핑이란 원래 ‘속이다, 사기치다’라는 ‘Spoof’의 의미를 가진다. 네트워크를 이용한 다양한 공격 중 IP 스푸핑은 아주 적극적이면서 고도의 공격 기술을 보유한 전문 해커들의 공격 행위로 분류하고 있다.

네트워크상에 존재하는 신뢰 호스트들은 접근 과정의 인증을 위하여 상호 IP 주소를 이용하고 있다. IP 스푸핑이란 인증 과정에 필요한 특정 호스트의 IP를 강탈해 정상적인 인증 과정을 수행하는 것을 의미한다. 아울러 실질적인 타겟 호스트를 공격하기 전 IP를 강탈한 해당 호스트를 다운시키기 위하여 서비스 거부 공격 등 자원 고갈 공격 등을 시도한다[11]. 이러한 전 과정은 <그림 1>에서 보이고 있다.

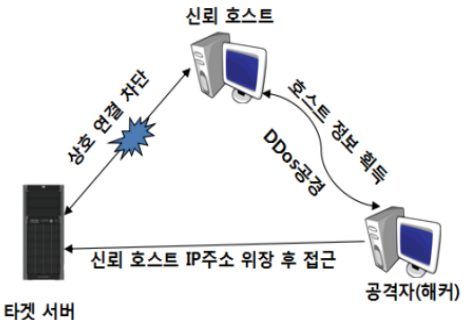

그림 1. IP 스푸핑 과정
Figure 1. A process of IP Spoofing

IP 스푸핑 공격은 향후 클라우드 서비스 환경에서 집중적으로 발생할 가능성이 아주 높다고 할 수 있다.

트레이스 백이란 네트워크상에 존재하는 송신자와 수신자 사이에 존재하는 라우터들의 IP를 추적하여 그 연결 경로 정보를 제공해 주는 프로그램이다. 즉, 특정 호스트가 네트워킹 작업을 수행하면서 최종 수신자까지 라우터들의 각 구간 경로에 해당하는 IP를 제공해 주는 프로그램이다[12]. 아울러 OTP는 무작위로 생성되는 난수를 이용한 일회용 패스워드를 의미하며, 네트워크상에서 이를 이용하여 사용자 인증 과정을 수행한다. 즉, 로그인 과정에 고정적인 패스워드를 사용하지 않고, 일회성 패스워드를 생성하여 동일한 패스워드의 반복 사용으로 발생할 수 있는 보안상의 취약점을 보완하고 있다.

IP 스푸핑 공격 탐지 및 대응과 관련한 트레이스 백 정보와 OTP에 기반한 기존 연구들은 서비스 가용성에 대한 문제를 안고 있다.[8-9, 12]

트레이스 백 정보와 OTP에 기반한 기존 연구들은 공격 탐지를 위한 비교 과정에서 트레이스 백 정보가 상이한 경우 매번 OTP를 생성하고 있다. 그러므로 이로 인한 연결 과정의 오버헤드를 초래할 수 있다. 본 논문에서는 과다한 OTP 생성 문제를 해결하기 위하여 유클리드 거리 좌표 값에 대한 임계 범위를 두고, 경우에 따라 OTP 생성과 암호화 과정을 병행 사용하도록 하였다[13].

본 논문에서는 트레이스 백 과정에서 생성되는 라우터들의 IP를 이용하여 유클리드 거리를 계산하고 유클리드 거리 값 분포도를 통한 임계치 값을 이용하여 정상적인 사용자 여부 판정과 이후 대응 과정을 수행하도록 하였다.

유클리드 거리는 두 점 사이의 거리를 계산할 때 일반적으로 사용하는 방법이다. 본 논문에서는 트레이스 백을 통하여 생성되는 라우터들의 IP 주소 값을 두 개의 쌍으로 설정하여 유클리드 거리 연산을 한 후 유클리드 공간을 정의 하여 인증 과정을 수행하도록 하였다. 아울러 유클리드 거리에 대응하는 노름을 유클리드 노름이라고 하는데, 직교 좌표계로 나타낸 점 p = (p1, p2,..., pn)와 q = (q1, q2,..., qn)가 존재할 때, 두 유클리드 노름을 이용한 두 점 p, q의 거리는 다음과 같이 계산할 수 있다[14-15].

유클리드 거리 좌표 유도식

$$\epsilon = \{R^2, L_E, d_E\}$$

$$R^2 = \{(p,q) | p,q \in R\}$$

L_E는 모는 직선의 집합

임의의 두 점 $p = (x_1, y_1), q = (x_2, y_2)$에 대해

$$d_E(p,q) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}$$

3. 제안 모델 동작과정

본 논문에서 제안하고 있는 사용자 인증 모델의 접근 처리 과정은 <그림 2>와 같다.

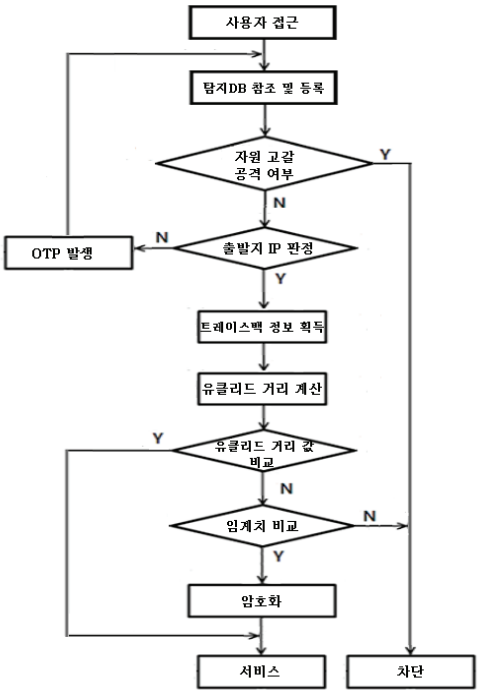

그림 2. 제안 모델의 사용자 인증 과정
Figure 2. A processing of user Authentication in the proposed model

먼저 클라우드 서비스 호스트에 대한 사용자 접근이 발생하면 공격 탐지를 위한 데이터베이스를 참조하여 해당 IP의 자원 고갈 공격 여부를 검사한다. 이는 IP 스푸핑 공격 과정에 있어 공격자가 기존의 신뢰 호스트의 IP를 공유할 수 없으므로 해당 신뢰 호스트를 무력화시키기 위한 공격을 시도하기 때문이다. 그러므로 자원 고갈 공격이 클라우드 네트워크상의 특정 호스트에 발생했다면 해당 정보를 클라우드상의 모든 호스트가 공유할 수 있도록 공격 탐지 데이터베이스에 등록하여 향후 동일한 공격에 능동적으로 대응할 수 있도록 하였다.

그 다음 사용자의 출발지 IP를 우선 비교 분석하여 클라우드 서비스를 구성하는 신뢰 호스트 여부를 판단한다. 만일 출발지 IP가 일치하지 않는 경우에는 OTP를 발생시켜 인증을 완료하면 탐지 데이터베이스에 새로운 접근 경로 등록을 하고, 인증을 실패하면 공격자 정보로 등록한다.

출발지 IP 분석을 통하여 해당 IP가 탐지 데이터베이스에 신뢰 호스트로 등록되어 있다면, 해당 IP에 대한 트레이스 백 정보를 획득하여 이를 기반으로 인증을 위한 유클리드 거리 정보를 계산한다.

기존의 논문에서는 트레이스 백 정보가 완전히 일치할 때만 서비스 작업을 수행하고 그렇지 못한 경우에는 일반적으로 OTP 전송을 통하여 재인증 과정을 수행한다. 그렇지만 이러한 기법은 잦은 OTP를 이용한 재인증 과정을 요구하기 때문에 이로 인한 오버헤드를 초래할 수 있다.

본 논문에서는 유클리드 거리 값 비교에서 완전 일치로 결과가 나오면 기존 방식과 같이 바로 서비스를 실시한다. 그렇지만 트레이스 백 정보를 분석하는 과정에서 일부의 IP 변경이 존재하더라도 본 논문에서는 유클리안 거리 값에 기반한 평균 임계치를 이용하기 때문에 OTP 재인증에 대한 오버헤드를 감소시킬 수 있다. 아울러 임계치 범위에 존재하면 암호화 과정을 통하여 서비스를 수행하고, 임계치를 벗어나면 바로 차단 작업을 수행하도록 하였다.

4. 실험 및 평가

본 논문의 실험을 위한 트레이스 백 정보는 본 연구자의 컴퓨터를 출발지로 하고 국내 임의의 지역에 존재하는 서버를 목적지로 하여 해당 정보를 <그림 3>, <그림 4>와 같이 획득하였다.

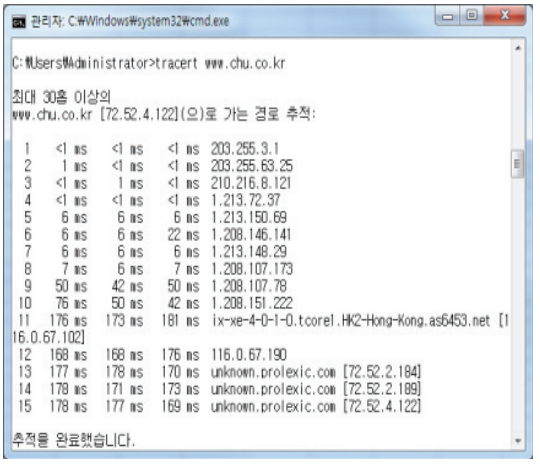

그림 3. 트레이스 백 정보 결과 1

Figure 3. Results-1 of traceback information

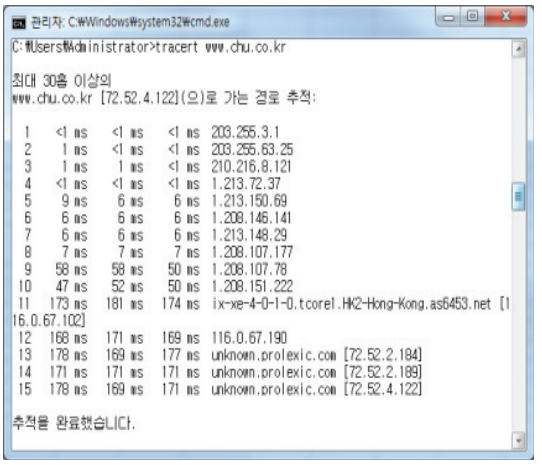

그림 4. 트레이스 백 정보 결과 2

Figure 4. Results-2 of traceback information

<그림 3>, <그림 4>의 트레이스 백 정보 결과를 보면, 정상적인 사용자가 동일한 IP를 이용한 접근이 발생했지만 8번째에 존재하는 라우터 IP가 동일하지 않다는 것을 알 수 있다. 이 경우 본 논문의 유클리안 기반의 임계치 분석 그래프를 통하여 동일한 결과를 보이기 때문에 OTP를 발생시키지 않고 서비스를 수행하도록 한다.

<그림 5>는 트레이스 백 정보를 이용하여 경유 라우터들의 IP를 직교 좌표로 나타낸 것이다.

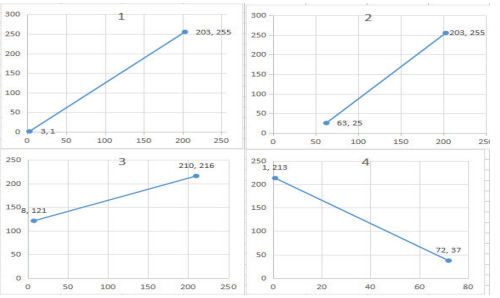

그림 5. IP 쌍을 이용한 거리 좌표

Figure 5. Two sets of coordinates Based IP

<그림 6>은 트레이스 백 정보를 이용하여 유클리드 거리를 계산한 값에 대한 표이다.

HOP개수	X1	X2	Y1	Y2	Euclidean distance.1
1	203	3	255	1	323.289
2	203	63	255	25	269.258
3	210	8	216	121	223.224
4	1	72	213	37	189.781
5	1	150	213	69	207.212
6	1	146	208	141	159.731
7	1	148	213	29	235.510
8	1	107	208	177	110.440
9	1	107	208	78	167.738
10	1	151	208	222	150.652
11	116	67	0	102	113.159
12	116	67	0	190	196.217
13	72	2	52	184	149.412
14	72	2	52	189	153.847
15	72	4	52	122	97.591

HOP개수	X1	X2	Y1	Y2	Euclidean distance.2
1	203	3	255	1	323.289
2	203	63	255	25	269.258
3	210	8	216	121	223.224
4	1	72	213	37	189.781
5	1	150	213	69	207.212
6	1	146	208	141	159.731
7	1	148	213	29	235.510
8	1	107	208	173	111.629
9	1	107	208	78	167.738
10	1	151	208	222	150.652
11	116	67	0	102	113.159
12	116	67	0	190	196.217
13	72	2	52	184	149.412
14	72	2	52	189	153.847
15	72	4	52	122	97.591

그림 6. 유클리드 거리 계산 과정

Figure 6. Euclidean distance calculation process

<그림 7>은 <그림 3>에 기반한 유클리드 거리 좌표 값 계산을 통하여 도출된 그래프이다.

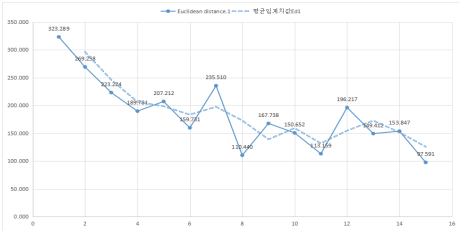

그림 7. 유클리드 거리 값 그래프 1
Figure 7. Graph-1 of Euclidean distance numerical values

<그림 8>은 <그림 4>에 기반한 유클리안 거리 값 계산을 통하여 도출된 그래프이다.

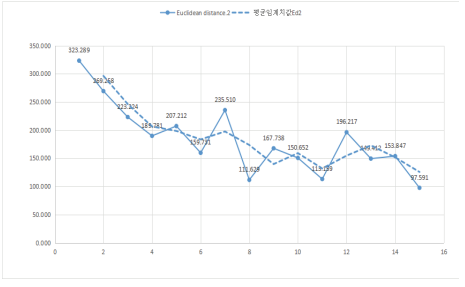

그림 8. 유클리드 거리 값 그래프 2
Figure 8. Graph-2 of Euclidean distance numerical values

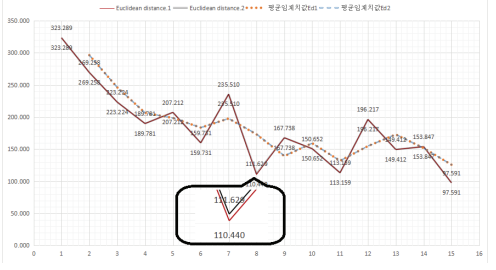

그림 9. 임계치 분석 그래프
Figure 9. Threshold analysis graph

<그림 9는> 유클리드 거리 값 계산을 통하여 도출된 <그림 7>과 <그림 8>을 통합시킨 결과를 나타내는 그래프이다. <그림 9>의 유클리안 거리 값은 8번째 경유 라우터에 차이를 보이지만 임계치를 나타내는 평균값 그래프에는 그 차이를 거의 보이지 않는다. 그러므로 이 경우에는 OTP를 발생시키지 않고 암호화 과정 등을 통한 서비스를 수행하기 때문에 서비스 가용성을 향상시킬 수 있다.

<그림 10>은 트레이스 백 정보가 일치 하지 않을 경우 그 결과를 유클리드 거리 값 계산을 통하여 도출한 표이다.

HOP개수	X1	X2	Y1	Y2	Euclidean distance.3
1	203	3	255	1	323.289
2	112	209	174	1	198.338
3	112	206	174	63	145.454
4	112	49	174	14	171.956
5	112	84	174	226	59.059
6	129	8	250	69	217.720
7	129	2	250	11	270.647
8	129	2	250	97	198.842
9	129	2	250	125	178.197
10	129	5	250	249	124.004
11	203	254	131	138	51.478
12	103	45	235	6	236.231
13	72	2	52	184	149.412
14	72	2	52	189	153.847
15	72	4	52	122	97.591

그림 10. 상이한 경로정보에 기반한 유클리드 거리 계산 과정
Figure 10. Euclidean distance calculation process based on different routing information

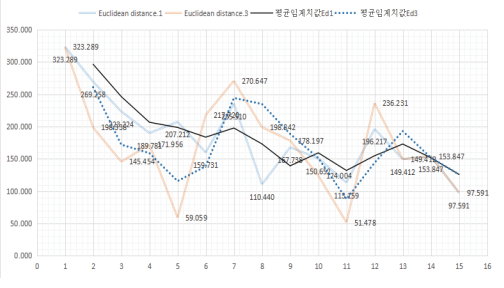

그림 11. <그림6>, <그림 10> 기반의 임계치 분석 그래프
Figure 11. Threshold analysis graph based on <Fig. 6> and <Fig. 10>

<그림 11>은 유클리드 거리 값 계산을 통하여 도출된 <그림 6>과 <그림 10>에 기반한 결과를 그래프로 통합시킨 결과이다. <그림 6>에 의한 그래프 결과는 트레이스 백 정보가 완전히 일치하거나 일부 경로 정보가 상이하더라도 임계치에 포함될 경우 <그림 9>와 같이 OTP를 발생하지 않는다. 그렇지만 트레이스 백 정보가 상이한 경우기존 연구에서는 임계치에 대한 비교 과정이 없기 때문에 한 곳이라도 상이한 경로 정보가 탐지되면 OTP를 발생시켜 이로 인한 오버헤드를 초래할 수 있다.

5. 결 론

오늘날 네트워크 환경은 빠르게 발전하고 있다. 본 논문은 이러한 네트워크 환경에 대하여 불법적인 접속이 발생할 경우 능동적이고 안정적인 서비스 수행이 가능하도록 하였다.

일반적인 트러스트 네트워크 환경에서 클라이언트의 서비스 요청에 대한 기존 탐지 방식은 트레이스 백 정보의 단순 비교를 통한 방식을 이용하고 있다. 그렇지만 이러한 탐지 방식은 정상적인 접근과 불법적인 접근에 대한 분석과정에서 빈번한 OTP 발생을 가져오면서 서비스 가용성을 저하시킬 수 있다.

본 논문은 이러한 OTP 과다 발생을 감소시키기 위하여 유클리안 거리 계산법을 이용하였다. 아울러 이를 통하여 트레이스 백 과정에서 획득 가능한 경유 라우터들의 IP 정보로 유클리안 거리 자료를 계산한 후 그래프로 나타내었다. 이는 향후 클라우드 서비스를 요청하는 클라이언트들의 정상 여부를 비교 분석하기 위함이다.

본 논문은 이렇게 생성한 그래프 분석으로 정상적인 클라이언트의 트레이스 백 정보가 완전하게 일치하지 않더라도 분석 그래프에 저장되어 있는 임계치 정보를 이용하여 재인증을 위한 OTP 발생이 없다. 또한 이 과정에서 발생할 수 있는 미세한 탐지 오류에 대비하여 암호화 기법을 사용하고 있기 때문에 잘 못 유출되는 자료에 대한 보안 문제도 해결하였다. 향후 연구 과제로는 유클리드 거리를 계산을 통한 탐지 속도와 기존의 탐지 속도를 비교 분석하여 서비스 가용성을 더욱 향상 시킬 수 있는 연구가 병행되어야 한다고 본다.

References

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

[2] 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.

[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] A. Lee, *Guideline for Implementing Cryptography in the Federal Government.* Nist SP 800-21.112, 1999.

[5] S. Gueron, *Advanced encryption standard (AES) instructions set.* White paper of Inter, 2008.

[6] X-F. Meng, and X-B. Ci, *Data management : Concepts, techniques and challenges*, School of Information, Renmin University of China, Beijing 100872, pp. 146-169, 2013.

[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] 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.

[9] 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.

[10] J. Heo, *Detecting abnormal SIP (Session Initiation Protocol) traffic using statistical distribution estimation.* Journal of KISS : Software and Applications Vol. 38, No. 11, pp. 606-612, Nov. 2011.

[11] Y. H. Shin, G. H Lim, and E. G. Im, *A Research on the possibility of ARP spoofing attack in SCADA System Based on TCP/IP environment.* Convergence security journal, Vol. 9, No. 3, pp. 9-17, 2009.

[12] M-H Kim, H-C Beak, S-W Hong, 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.

[13] W. C. Hong, K. W. Lee, S. J. Kim, and D. H. Won, *Vulnerabilities andlysis of the OTP implemented on a PC*, DOI; 10.3745/KIPSTC. 2010.17C.4.361.

[14] S. Li, and S. G. Kang, *Design of 3-dimensional cross-lattice signal constellations with increased compactness,* Journal of the Korea Institute of Information and Communication Engineering, Vol. 20, No. 4, pp. 715-720 Apr. 2016.

[15] M-S Kim, J-H Kim, J-H Wo, L-S Lee and B-H Kim, *A function of a variety of distance in accordance with the definition of a regular polygon,* The Korean Soc. Math. Ed. Proceedings of the 47th National Meeting of Math. Ed. pp. 4-5, pp. 259-268, Nov. 2011.

유클리드 거리 기반의 OTP 재인증 감소 모델

유양[1], 백현철[2], 박재홍[1], 김상복*[1]
[1]*경상대학교 컴퓨터과학과*
[2]*경남도립남해대학 스마트융합정보과*

요 약

오늘날 정보통신 기술은 빅 데이터 서비스를 위한 클라우드 환경으로 빠르게 발전하고 있다. 이러한 네트워크 환경 변화는 온라인상으로 이루어지는 정보의 상호 교환 과정에 중요 정보 자료에 대한 보호 기능을 한층 요구하고 있는 상황이다. 네트워크 기반의 정보 보호에는 일반적으로 불법적인 접근에 대한 탐지 기법과 OTP를 이용한 인증 기법, 암호화 기법이 사용되고 있다. 그렇지만 이러한 기법들은 다양한 기법을 이용한 공격에 취약점을 보이고 있다. 특히 고도의 불법적인 접근 기술을 보유하고 있는 공격자들은 일반적으로 IP 스푸핑 공격을 빈번하게 시도하고 있다. 즉, 상호 신뢰 관계에 있는 클라우드 상의 호스트 정보를 이용하여 불법적인 공격을 시도하기 때문에 클라우드 서비스 환경에서는 이러한 신뢰 관계를 이용한 공격 빈도가 더욱 증가할 수 있다. 본 논문은 클라우드 환경에서 서비스 접근성을 향상시키기 위하여 기존의 트레이스 백 정보의 분석 과정에 수학적 유클리드 거리 계산식을 이용하였다. 본 논문의 유클리드

거리 좌표는 각 홉이 보유하고 있는 IP 값을 각 두 개씩 짝을 지어 거리 좌표로 사용하였다. 그 다음 이들 좌표 값을 그래프로 나타낸 후 이에 대한 변이 추적을 하였다. 아울러 해당 변이 정보의 분석 후 OTP 전송이나 암호화 과정을 수행하기 때문에 재인증 과정에서 요구되는 OTP 전송에 대한 오버헤드를 감소시킬 수 있었다.

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

Hyun Chul Baek received the Ph.D. degree in the Department of Computer Science from Gyeongsang National University in 2003. He was a chairman in the Committee of Computer System technology at The Korea Association of Regional Public Hospital in 2007. He has been a professor in the Department of smart convergence Information, Gyeongnam Provincial Namhae College since 2013. His current research interests include network, network security, encryption, bigdata security, cloud computing. He is a member of the KKITS.

E-mail address: dosi_gas@lycos.co.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

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