JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 25, No. 9, pp. 2471-2478, Sep. 2024

Check for updates

양자 공격의 대응되는 격자 기반 사용자 인증 암호 프로토콜의 보안 취약점 분석

이 정 훈[1] · 최 윤 성[2*]
[1]인제대학교 컴퓨터공학부 학사과정
[2]인제대학교 AI소프트웨어 학부 조교수

Security Vulnerability Analysis of Corresponding Lattice-Based Cryptography Protocols for User Authentication Against Quantum Attacks

Jung-Hun Lee[1] · Youn-Sung Choi[2*]

[1]Bachelor's Course, Department of Computer Engineering, Inje University, Gimhae 24631, Korea
[2]Assistant Professor, Department of AI & Software, Inje University, Gimhae 24631, Korea

[요 약]

PC와 IT 기술의 발전으로 인해서 데이터의 양이 증가함에 따라서 클라우드 컴퓨팅이라는 개념이 등장하였다. 클라우드 컴퓨팅의 등장으로 시간과 장소에 제약을 받지 않고, 동일한 데이터에 접근하거나 사용하는 것이 가능하게 되었다. 이 과정에서 통신 간의 정보가 인증되지 않은 사용자는 공개 클라우드 서버에 접근하지 못하도록 하고 클라우드를 사용하는 사용자의 개인정보가 유출되지 않도록 보안 점검 또한 중요하게 관리해야 할 부분이 되었다. 그중 공개 클라우드 환경에서 양자 공격을 막을 수 있는 격자 암호 기반의 사용자 암호 인증 프로토콜을 Naveed Khan 등이 제안하였다. 제안된 격자 기반의 사용자 암호 인증 프로토콜에는 다양한 취약점이 존재했으며, 본 논문에서는 Naveed Khan이 제안한 암호 인증 프로토콜의 취약점을 분석하여 Offline Password Guessing Attack, Lack of Perfect Forward Secrecy, Dos Attack의 공격에 취약하다는 것과 암호의 비효율성과 설계 과정에서 일어나는 설계 오류를 밝혀냈다.

[Abstract]

With advancements in PC(Personal Coumputer) and IT(Information Technology) and an increase in data volume, the concept of cloud computing has emerged. The advent of cloud computing has enabled access to and/or the utilization of the same data regardless of time and location. Therefore, security checks have become crucial for preventing unauthorized access to public cloud servers and protecting the personal information of cloud users. Naveed Khan et al. proposed a grid password–based user authentication protocol that can prevent quantum attacks in a public cloud environment. However, the protocol exhibits various vulnerabilities. Therefore, this study analyzed these vulnerabilities, revealing the susceptibility of the aforementioned proposed protocol to offline password guessing attacks, lack of perfect forward secrecy, and DoS(Denial of Service) attacks and highlighting its inefficiency and password design errors.

색인어 : 클라우드 컴퓨팅, 공개 클라우드 서버, 양자 암호, 사용자 인증 암호 프로토콜, 격자 암호
Keyword : Cloud Computing, Public Cloud Server, Quantum Cryptography, User Authentication, Lattice Encryption

http://dx.doi.org/10.9728/dcs.2024.25.9.2471

Received 19 July 2024; **Revised** 06 September 2024
Accepted 20 September 2024

***Corresponding Author; Youn Sung Choi**

Tel: +82-55-320-3206
E-mail: cys2020@inje.ac.kr

Ⅰ. 서 론

인터넷과 PC의 발전으로 컴퓨터 간의 통신 기술은 지속적인 발전을 거듭하여 많은 양의 데이터 전송이 가능하게 되었고, 데이터의 양과 사용자가 관리해야 할 데이터의 개수가 증가하면서 고속화된 인터넷 속도를 지원하고 사용자들 간의 데이터를 공유할 수 있는 클라우드 컴퓨팅이 등장하였다.

클라우드 컴퓨팅은 컴퓨팅 리소스를 인터넷을 통해 서비스로 사용할 수 있는 주문형 서비스를 의미하며, 기업에서 직접 리소스를 조달하거나 구성, 관리할 필요가 없으며 사용한 만큼만 비용을 지불하면 되는 구조로 구성되어 있다. 간단히 말해서 클라우드 컴퓨팅은 네트워크를 사용하여 사용자가 대여 컴퓨팅 서비스를 요청하고 접근하는 클라우드 플랫폼에 연결한다. 이후. 중앙 서버는 클라이언트 기기와 서버 간의 모든 통신을 처리하여 데이터 교환을 가능하게 한다[1]-[4].

이러한 특징을 활용하여 확장성과 유연성을 가지면서 비용을 절감할 수 있으며, 높은 가용성과 안정성 및 협업과 융합의 가능성이 존재한다. 또한 빠른 서비스의 제공 속도로 인하여 인프라 구축과 설정에 드는 시간을 단축하고 기업의 시장 진입을 가속화 할 수 있다는 점과 자동화와 관리가 용이하다는 장점이 존재하기 때문에, 웹 애플리케이션 및 모바일 앱 호스팅이나 데이터 분석 및 빅데이터 처리, 딥러닝 및 인공지능 연구, 영상 스트리밍 및 게임 서버 호스팅과 IOT 분야에서도 활용되고 있다. [3]-[6]

클라우드 컴퓨팅 과정에서 클라이언트와 중앙 서버 간 통신 과정에서 인증되지 않은 사용자인 공격자가 인증된 사용자인 피해자의 공개 클라우드 서버에 악의적으로 접근하여 통신하고 있는 정보가 탈취하지 못하도록 보안 및 개인정보 보호 기능 또한 중요해졌으며, 이 정보를 안전하게 보호하는 방법에 대하여 연구가 필요하다[5]-[8].

Naveed Khan 등은 공개 클라우드 환경에서 일어날 수 있는 양자 공격을 방어할 수 있는 사용자 인증 프로토콜을 제안하였다. 해당 프로토콜은 사용자가 ID와 PW를 입력하여 공개 클라우드 서버로 전송하면 서버에서 난수를 생성하여 해시값을 생성해서 사용자에게 전송하고 전송받은 데이터를 사용자가 다시 한번 더 연산을 수행하고 비교하여 인증을 진행한다. 그러나, 본 연구에서는 Naveed Khan 등이 제안한 사용자 암호 인증 프로토콜에서 Offline Password Guessing Attack, Lack of Perfect Secrecy, DOS Attack 취약하다는 것을 발견하고, 제안된 사용자 암호 인증 프로토콜의 설계 과정에서의 설계 오류와 해당 프로토콜의 인증 진행 과정에서의 비효율성을 밝혀냈다[2],[10].

따라서 본 논문의 연구 목표는 먼저 Naveed Khan 등이 제안한 사용자 인증 암호 프로토콜의 동작 과정을 분석하고 해당 프로토콜의 진행 과정이 앞서 언급한 3가지 취약점인 Offline Password Guessing Attack, Lack of Perfect Secrecy, DOS Attack의 취약성과 비효율성 및 설계 오류를 증명하는 것으로 결론을 맺는다.

Ⅱ. 관련 연구

2-1 Homomorphic Encryption

동형암호(Homomorphic Encryption)은 그림 1과 같이 평문과 암호문의 동형(Homomorphic) 성질로 인해 암호문 상태에서도 연산이 가능한 차세대 암호 기술이다.

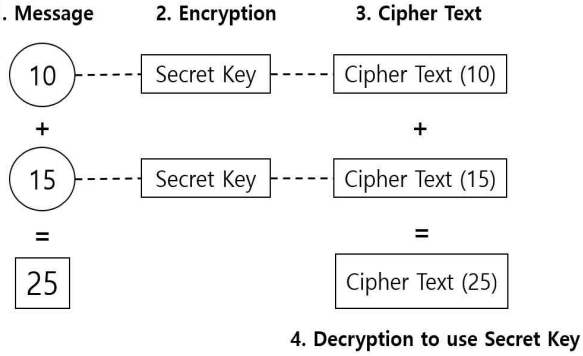

그림 1. 동형암호
Fig. 1. Homomorphic encryption

데이터를 기존 암호 알고리즘을 통해 비식별화하는 경우 클라우드에서 암호화된 데이터에 대한 연산이 불가능한 반면, 동형암호를 활용하면 암호화된 데이터에 대해서 복호화를 진행하지 않고 암호화가 되어있는 상태에서 연산을 수행할 수 있으므로 민감정보를 안전하게 보호하면서도 유용하게 데이터를 활용할 수 있다[2],[13].

2-2 Lattice-Based Cryptography

Lattice-Based Cryptography (격자 기반 암호화)는 구성 자체 또는 보안 증명에서 격자를 포함하는 암호화 기본 형식의 구성에 대한 일반적인 용어로 설명할 수 있다. 격자 기반 구조는 양자 내성 암호화의 중요한 표준을 지원하며, 이론적으로 RSA, Diffie-Hellman 또는 타원 곡선 암호와 같이 더 널리 사용되고 알려진 공개 키 암호와 달리 일부 격자 기반 구조는 고전 컴퓨터와 양자 컴퓨터 모두를 대상으로 한 공격에 내성이 있으며, 잘 연구된 특정 계산 격자 문제가 효율적으로 해결될 수 없다는 가정하에서 많은 격자 기반 구조가 안전한 것으로 간주 된다[2],[13].

Ⅲ. 프로토콜 동작 분석

Naveed Khan의 논문을 보면, 제안된 프로토콜을 분석하기 위해서 사용된 기호 및 정보는 표 1과 같다. 해당 논문에서 사용된 프로토콜은 크게 2가지의 단계로 구성되었으며, 동작

표 1. 프로토콜의 기호 정의
Table 1. Symbols and description

Symbols	Description
U	User
PCS	Cloud server
ID_U	Identify of user
PW_U	Password of user
r_s , r_{s1}	The random numbers of cloud server
r_U	A random number of user
χ_β	Gaussian distribution
∂, γ, ρ	Gaussian distribution samples
q	Odd prime number
i	Integer
S	The secret key of the cloud server
PK_S	The public key of the cloud server
$\|\|$	Concatenation
$h(.)$	Hash function

분석은 사용자 등록 단계와 사용자 로그인 인증과정의 순서대로 진행한다.

3-1 사용자 등록 과정

프로토콜을 사용하기 위해서 사용자 등록을 진행하게 되는데 아래의 그림 2와 같다.

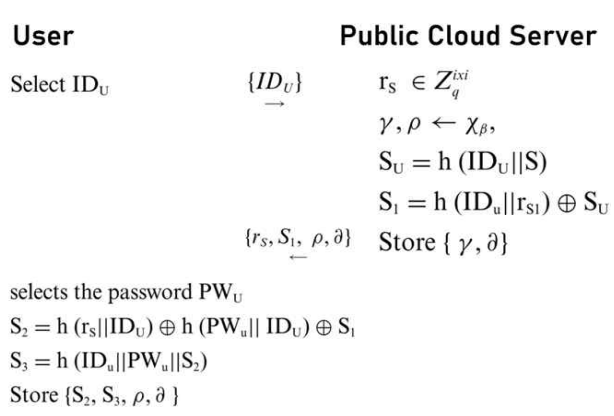

그림 2. 사용자 등록과정
Fig. 2. Login registration procedure

그림 2를 보면 *User*는 사용할 ID_U 를 공개 클라우드 서버로 전송하게 되고, 공개 클라우드 서버는 ID_U를 수신하여 $r_s \in Z_q^{ixi}$를 만족하는 난수를 생성한다. 이때, 사용되는 q는 $q \bmod 2i = 1$을 만족하며 공개 클라우드 서버는 비밀키 S를 생성한다.

$$S \Rightarrow e \leftarrow \chi_\beta \Rightarrow f(x) = \frac{1}{\sqrt[\sigma]{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})} \quad (1)$$

사용자의 ID_U와 난수 r_s를 바탕으로 보안을 강화하기 위해서 해시함수인 $h(.)$를 사용하여 *User*의 비밀키인 S_U를 생성한다. 이후, S_U를 사용하여 S_1을 생성한 다음, 클라우드 서버에 $\{\gamma, \partial\}$를 저장한다.

$$S_U = h(ID_U \| S) \quad (2)$$

$$S_1 = h(ID_U \| r_{s1}) \oplus S_U \quad (3)$$

공개 클라우드 서버는 S_1의 값을 구한 뒤, 다시 *User*에게 PW_U를 받기 위해서 $\{r_s, S_1, \rho, \partial\}$의 값을 전송하면 *User*는 PW_U를 입력하게 되고 입력된 PW_U는 전송받은 $\{r_s, S_1, \rho, \partial\}$의 값을 이용하여 $\{S_2, S_3, \rho, \partial\}$값을 *User*가 저장한다.

$$S_2 = h(r_s \| ID_U) \oplus h(PW_U \| ID_U) \oplus S_1 \quad (4)$$

$$S_3 = h(ID_U \| PW_U \| S_2) \quad (5)$$

3-2 사용자 인증 과정

사용자의 로그인 인증과정은 그림 3, 4, 5와 같이 진행되며 사용자 등록과정에서 각각 저장된 값을 비교하고 활용한 연산을 이용하여 사용자의 인증을 그림 3과 같이 수행한다.

그림 3. 사용자 인증 과정 (1)
Fig. 3. Login and authentication procedure (1)

*User*는 등록과정에서 저장한 S_2의 값을 이용하여 새로운 S_3^*의 값을 생성 후, 공개 클라우드 서버에 저장된 S_3의 값과 비교한 후 일치하면 프로토콜을 계속 진행하고 일치하지 않는다면 연결을 종료한다.

$$S_3^* = h(ID_U^* \| PW_U^* \| S_2) \quad (6)$$

$$S_3^*? = S_3 \quad (7)$$

S_3^*가 S_3와 일치하면 인증을 완료하고 *User*가 $r_U \in Z_q^{ixi}$를 만족하는 난수 r_U를 생성하고 등록과정에서 저장된 ρ를 사용하여 아래의 수식과 같이 M 값을 계산하여 공개 클라우드 서버로 전송한다.

$$M = r_s \bullet r_U + 2\rho \tag{8}$$

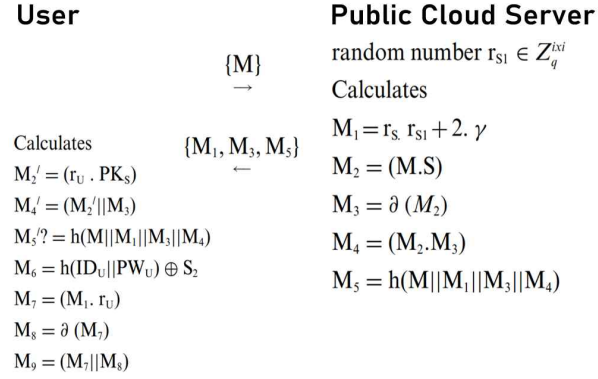

그림 4. 사용자 인증 과정 (2)
Fig. 4. Login and authentication procedure (2)

공개 클라우드 서버는 그림 4와 같이 $r_{s1} \in Z_q^{ixi}$를 만족하는 새로운 난수 r_{s1}을 생성하고 *User*에게 전송받은 M값을 바탕으로 아래와 같이 연산한 이후, $\{M_1, M_3, M_5\}$의 값을 *User*에게 전송한다.

$$M_1 = r_s \bullet r_{s1} + 2 \bullet \gamma \tag{9}$$

$$M_2 = (M \bullet S) \tag{10}$$

$$M_3 = \partial(M_2) \tag{11}$$

$$M_4 = (M_2 \bullet M_3) \tag{12}$$

$$M_5 = h(M \parallel M_1 \parallel M_3 \parallel M_4) \tag{13}$$

*User*는 공개 클라우드 서버에서 $\{M_1, M_3, M_5\}$의 값을 수신한 다음, 클라우드 서버의 공개키 PK_s와 이전 과정에서 수행되었던 난수 r_U를 활용하여 M_2'를 계산하고 M_2'를 포함한 연산을 다음과 같이 수행한 후 *User*의 비밀키 S_{KU}를 생성한 다음, 공개 클라우드 서버에 $\{M_{10}, M_8, M_{11}\}$을 송신한다.

$$M_2' = (r_U \bullet PK_s) \tag{14}$$

$$M_4' = (M_2' \parallel M_3) \tag{15}$$

$$M_5' ? = h(M \parallel M_1 \parallel M_3 \parallel M_4) \tag{16}$$

$$M_6 = h(ID_U \parallel PW_U) \oplus S_2 \tag{17}$$

$$M_7 = (M_1 \bullet r_U) \tag{18}$$

$$M_8 = \partial(M_7) \tag{19}$$

$$M_9 = (M_7 \parallel M_8) \tag{20}$$

$$M_{10} = h(M \parallel M_8 \parallel M_9 \parallel M_1 \parallel M_3 \parallel M_4 \parallel M_2) \oplus ID_U \tag{21}$$

$$M_{11} = h(ID_U \parallel M_6 \parallel M_{10} \parallel M \parallel M_8 \parallel M_9 \parallel M_1 \parallel M_3 \parallel M_2' \parallel M_5) \tag{22}$$

$$S_{KU} = h(ID_U \parallel M_{10} \parallel M \parallel M_8 \parallel M_9 \parallel M_{11} \parallel M_1 \parallel M_3 \parallel M_2' \parallel M_5) \tag{23}$$

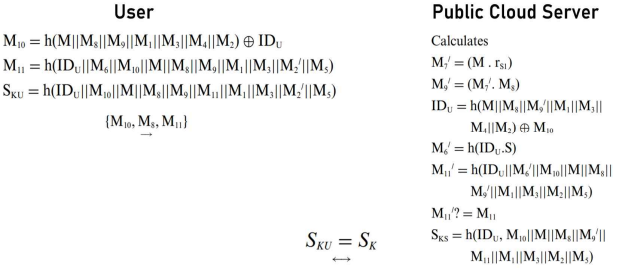

그림 5. 사용자 인증 과정 (3)
Fig. 5. Login and authentication procedure (3)

그림 5와 같이 $\{M_{10}, M_8, M_{11}\}$을 수신받은 공개 클라우드 서버는 아래와 같이 재계산하여 공개 클라우드의 비밀키 S_{KS}를 생성하여 S_{KU}와 비교하여 인증 절차를 완료한다.

$$M_7' = (M \bullet r_{s1}) \tag{24}$$

$$M_9' = (M_7' \bullet M_8) \tag{25}$$

$$ID_U = h(M \parallel M_8 \parallel M_9' \parallel M_1 \parallel M_3 \parallel M_4 \parallel M_2) \oplus M_{10} \tag{26}$$

$$M_6' = h(ID_U \bullet S) \tag{27}$$

$$M_{11}' = h(ID_U \parallel M_{10} \parallel M \parallel M_8 \parallel M_9' \parallel M_1 \parallel M_3 \parallel M_2 \parallel M_5) \tag{28}$$

$$M_{11}' ? = M_{11} \tag{29}$$

$$S_{KS} = h(ID_U \parallel M_{10} \parallel M \parallel M_8 \parallel M_9' \parallel M_{11} \parallel M_1 \parallel M_3 \parallel M_2 \parallel M_5) \tag{30}$$

$$S_{KS} \leftrightarrow S_{KU} \tag{31}$$

Ⅳ. 사용자 암호 인증 프로토콜 취약점 분석

4-1 Offline Password Guessing Attack

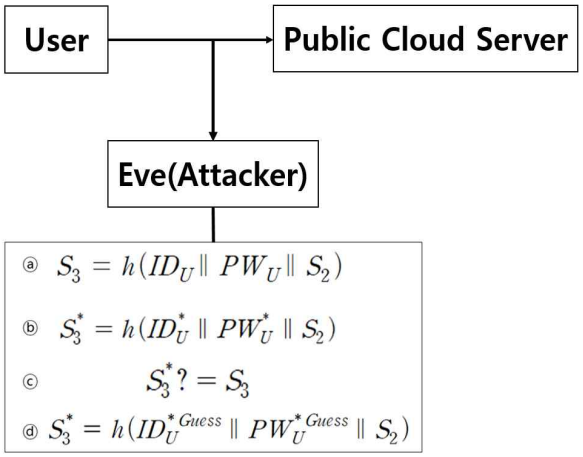

그림 6. 오프라인 패스워드 추측 공격
Fig. 6. Offline password guessing attack

Offline Password Guessing Attack은 공격 대상자의 패스워드를 추측한 공격자는 프로토콜의 정상적인 메시지를 도청하고 저장한 후, 저장된 메시지를 이용하여 추측에 대한 검증을 오프라인으로 반복한다. 그림 6과 같이 $User$는 ID_U를 입력하면 공개 클라우드 서버에서 $User$가 전송한 PW_U를 요청하게 되는데 요청에 따라서 PW_U를 입력한 후 공개 클라우드 서버에서는 $User$의 등록 정보를 확인하는 절차로 인증이 진행된다. 이때 공격자가 공개 클라우드에 저장된 정보와 인증 절차를 진행하는 과정에서 공격자가 획득한 정보를 사용해서 $User$의 ID_U와 PW_U의 값을 유추할 수 있는 가능성이 존재한다. 해당 시스템의 프로토콜 진행 과정에서 사용자가 입력한 ID_U와 PW_U를 이용하여 생성한 $h(ID_U^* \| PW_U^* \| S_2)$를 S_3^*와 비교하고 $User$가 입력한 ID_U^*와 PW_U^* 값의 유효성을 검사한 다음, 현재 등록된 ID_U^*와 PW_U^* 값이 해당 $User$의 것과 일치하는지 확인하는 과정을 거친다. 하지만 공격자는 여기서 S_3^*의 값을 애용하여 로그인 정보를 다시 구성할 수 있게 되는데 여기서 공격자가 재구성한 S_3^*의 값은 ID_U^*와 PW_U^*를 제외한 모든 정보를 획득할 수 있게 된다. 처음에 $User$가 입력하는 ID_U^*와PW_U^*의 값은 $User$가 기억하고 있어야 하는 정보이므로 일정 길이의 문자열과 숫자로 구성된다는 것을 알 수 있다. 이러한 점을 이용하여 공격자는 무작위 패스워드 입력을 하면 경우의 수가 많지 않은 짧은 길이의 문자열로 ID_U^*와 PW_U^*를 생성하고 등록하기 때문에 경우의 수가 매우 적다. 따라서 본 연구에서는 해당 인증 프로토콜 시스템에서 Offline Password Guessing Attack에 취약하다는 것을 밝혀냈다[7],[13].

4-2 Lack of Perfect Secrecy

- Value Known to the attacker

$M, M_1, M_3, M_5, M_8, M_{10}, M_{11}$

- Value unknown to the attacker

M_2, M_4, M_9

- Calculate M_2, M_4, M_9

① $M_7 = (M_1 \cdot r_U)$ – Encryption
② $M_8 = \partial(M_7)$ – Decryption of M_7
③ $M_9 = (M_7 \| M_8)$ – Encryption to use M_7, M_8
$\therefore M_9 = ((M_1 \cdot r_U) \| \partial(M_1 \cdot r_U))$

---

① $M_2 = M \cdot S$ – Encryption
② $M_3 = \partial(M_2) = \partial(M \cdot S)$ – Decryption of M_2
③ $M_4 = (M_2 \cdot M_3)$ Encryption to use M_2, M_3
$\therefore M_4 = (M_2 \cdot M_3) = (M \cdot S) \cdot M_3$
$= (M \cdot S) \cdot \partial(M \cdot S)$

$S_{KU} = h(ID_U \| M_{10} \| M \| M_8 \| M_9 \| M_{11} \| M_1 \| M_3 \| M_2' \| M_5)$

그림 7. 인증 프로토콜에서 일어날 수 있는 공격자의 역산 과정
Fig. 7. Lack of perfect secrecy

Lack of Perfect Secrecy는 특정한 비밀키로 데이터를 암호화 하는 것을 의미하는데, 그림 7을 보면$User$의 로그인 인증과정에서 비밀키 S의 값을 공격자가 알고 있다면, 해당 프로토콜은 매우 취약하다.

프로토콜의 인증과정에서 공격자가 알 수 있는 값은 $M, M_1, M_3, M_5, M_8, M_{10}, M_{11}$이다. 여기서 마지막에 S_{KU}의 값을 구하게 되는데, 이 과정에서 공격자가 알 수 없는 값은 M_2, M_4, M_9의 값이 된다. 그러나 이 또한 인증과정에서 알 수 있게 되는데 $M_9 = (M_7 \| M_8)$에서 아래와 같이 표현할 수 있다.

$$M_9 = ((M_1 \cdot r_U) \| \partial(M_1 \cdot r_U)) \quad (32)$$

M_2의 값 또한 $M \cdot S$로 표현이 가능하고 M_4의 값 또한 계산이 가능해지고 세션 키를 획득하게 된다.

$$M_4 = (M_2 \cdot M_3) = (M \cdot S) \cdot M_3 = (M \cdot S) \cdot \partial(M \cdot S) \quad (33)$$

따라서 공격자가 비밀키 S의 값을 알고 있다고 가정하면 Lack of Perfect Secrecy를 만족하지 못한다[5],[6].

4-3 인증 프로토콜의 비효율성

$$M_2 = (M \bullet S) \quad \boxed{\text{Encryption (1)}} \quad M_7 = (M_1 \bullet r_U)$$

$$M_3 = \partial(M_2) \quad \boxed{\text{Decryption}} \quad M_8 = \partial(M_7)$$

$$M_4 = (M_2 \bullet M_3) \quad \boxed{\text{Encryption (2)}} \quad M_9 = (M_7 \| M_8)$$

그림 8. 프로토콜의 인증과정에서 일어나는 암호화 및 복호화
Fig. 8. Encryption and decryption that occurs during the authentication process of the protocol

해당 시스템의 인증 프로토콜의 과정에서 그림 8을 보면 M_2의 값을 구한 뒤 다시 M_3을 구하기 위하여 M_2의 값을 사용한다. 그리고 M_4를 구하기 위해서 M_2와 M_3의 값을 활용한다. 여기서 비효율적인 문제가 존재하는데, M_2의 값을 $M_2 = (M \bullet S)$라는 수식을 통하여 구한 뒤 $M_3 = \partial(M_2)$이라는 수식을 거쳐 M_4의 값을 구한다. 여기서 M과 S의 값을 활용하여 M_2의 값으로 암호화를 진행한 이후, 다시 M_3에서 복호화를 거치고 M_4의 값으로 다시 암호화를 진행한다. 이 과정에서 M_2의 값으로 암호화를 한 이후에 다시 M_3의 값을 연산하기 위해서 암호화된 M_2의 값을 복호화한다. M_7 또한, M_7의 값을 구한 뒤 다시 M_8을 구하기 위하여 M_7의 값을 사용한다. 그리고 M_9를 구하기 위해서 M_7과 M_8의 값을 활용한다. 여기서 비효율적인 문제가 존재하는데, M_7의 값을 $M_7 = (M_1 \bullet r_U)$라는 수식을 통하여 구한 뒤 $M_8 = \partial(M_7)$이라는 수식을 거쳐 M_8의 값을 구한다. 여기서 M_1과 r_U의 값을 활용하여 M_7의 값으로 암호화를 진행한 이후, 다시 M_8에서 복호화를 거치고 M_9의 값으로 다시 암호화를 진행한다. 이 과정에서 M_7의 값으로 암호화를 한 이후에 다시 M_8의 값을 연산하기 위해서 암호화된 M_7의 값을 복호화하므로 해당 시스템의 인증 프로토콜 절차가 비효율적이라는 사실을 알 수 있다. 해당 시스템의 인증 프로토콜은 복잡한 암호학적 연산을 진행하는데 이러한 연산이 많은 경우에는 프로토콜의 성능이 저하 될 수 있다는 단점이 존재한다[2].

4-4 DOS Attack

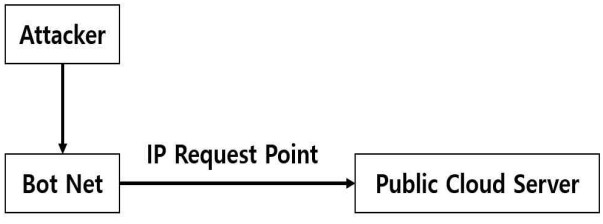

그림 9. Dos 공격
Fig. 9. Dos attack

DoS (Denial of Service) 공격은 인터넷 서비스를 사용할 수 없게 만드는 형태의 공격으로, 웹사이트, 서버, 네트워크, 애플리케이션 등을 목표로 한다. 이러한 공격은 트래픽 과부하, 리소스 고갈, 프로그램 취약점 등을 이용하여 시스템을 공격하며, 주로 정상적인 사용자들의 접속을 방해하여 서비스를 마비시키는 것을 목표로 한다. 따라서 해당 서비스는 다운된 것처럼 보이거나 사용할 수 없는 상태가 될 수 있다[6].

해당 시스템의 전체적인 등록과정과 인증 절차를 확인해 보면 사용자의 비밀키와 클라우드 서버의 비밀키를 마지막에 비교하는데 앞선 과정에서 복잡한 암호학적 연산을 하고 있으며, 인증과정 또한 M_5,M_{11}을 제외하고 인증을 진행하지 않는다. 그림 9와 같이 공격자의 입장에서 해당 프로토콜은 복잡한 연산을 거치기 때문에 데이터의 전송량이 증가한다면 공개 클라우드 서버의 네트워크 트래픽 대역폭 소모를 초래할 수 있을 것이다. 따라서 공격자가 악의적으로 많은 양의 데이터를 지속적으로 전송하게 된다면 프로토콜이 실행되는 환경의 공개 클라우드 서버는 리소스의 부족을 고려하지 않을 수 없다. 따라서 해당 시스템의 인증 프로토콜은 DOS Attack에 취약하다는 사실을 알 수 있다.

4-5 사용자 인증 암호 프로토콜 설계오류

Naveed.Khan 등이 제안한 프로토콜은 공개 클라우드 환경에서의 양자 공격에 대한 방어가 가능한 새로운 암호 인증 프로토콜이다. 그러나 제안한 프로토콜의 사용자 등록과 인증 절차에서 암호 알고리즘의 설계오류를 발견했다. 처음 $User$가 PW_U를 입력하면 다음과 같은 수식으로 S_2를 생성하는데 아래와 같다.

$$S_2 = h(r_S \| ID_U) \oplus h(PW_U \| ID_U) \oplus S_1 \quad (34)$$

그리고 등록 절차를 거쳐서 인증 절차를 확인해 보면 M_6에서 설계 오류를 확인할 수 있다.

$$M_6 = h(ID_U \| PW_U) \oplus S_2 \quad (35)$$

S_2에서 $User$의 $h(ID_U \| PW_U)$로 계산을 수행하였는데 이후 M_6에서는 $h(PW_U \| ID_U)$의 값으로 연산을 수행하였다. 이렇게 되면 S_2와 M_6의 값이 일치하지 않아 연산이 불가능하게 되고 더 이상 인증 절차를 수행할 수 없게 된다. 따라서 Naveed.Khan 등이 제안한 프로토콜은 설계 과정에서 오류가 있었다는 것을 확인할 수 있다. 만약, 연산이 가능하다고 하더라도 설계 과정에서의 오류가 있었으므로 설계 오류에 해당한다.

V. 결 론

Naveed Khan등이 제안한 프로토콜은 공개 클라우드 환경에서의 양자 공격에 대비할 수 있는 격자 암호 기반의 새로운 사용자 인증 암호 프로토콜을 제안했다. 해당 프로토콜을 복잡한 암호학적 연산과 여러 차례의 인증을 통하여 보안성을 높이고 검증되었다고 주장하지만 본 연구는 제안한 프로토콜을 분석하여 Offline Password Attack, Lack of perfect secrecy, Dos Attack의 취약성과 해당 시스템의 비효율성 및 설계 오류를 발견하였다. 본 연구 결과를 바탕으로 공개 클라우드 환경에서의 양자 공격에 대응할 수 있는 사용자 암호 인증 프로토콜에서 더욱 향상된 보안성과 취약성을 감소 및 신뢰성을 향상시킨 새로운 암호 인증 프로토콜을 설계할 수 있을 것으로 예상된다.

감사의 글

본 연구는 2024년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력 기반 지역혁신 사업의 결과입니다. (2021RIS-003)

참고문헌

[1] B. Godavarthi, N. Narisetty, K. Gudikandhula, R. Muthukumaran, D. Kapila, and J. V. N. Ramesh, “Cloud Computing Enabled Business Model Innovation,” *The Journal of High Technology Management Research*, Vol. 34, No. 2, 100469, November 2023. https://doi.org/10.1016/j.hitech.2023.100469

[2] N. Khan, J. Zhang, I. Ullah, M. S. Pathan, and H. Lim, “Lattice-Based Authentication Scheme to Prevent Quantum Attack in Public Cloud Environment,” *Computers, Materials & Continua*, Vol. 75, No. 1, pp. 35-49, February 2023. https://doi.org/10.32604/cmc.2023.036189

[3] P. Cheng, Y. Chen, M. Ding, Z. Chen, S. Liu, and Y.-P. P. Chen, “Deep Reinforcement Learning for Online Resource Allocation in IoT Networks: Technology, Development, and Future Challenges,” *IEEE Communications Magazine*, Vol. 61, No. 6, pp. 111-117, June 2023. https://doi.org/10.1109/MCOM.001.2200526

[4] J. Primbs and M. Menth, “OIDC^2: Open Identity Certification With OpenID Connect,” *IEEE Open Journal of the Communications Society,* Vol. 5, pp. 1880-1898, 2024. https://doi.org/10.1109/OJCOMS.2024.3376193

[5] J. Kwon, S. Hong, and Y. Choi “Security Analysis of Remote Healthcare System in Cloud-based IoT Environment,” *Journal of Korea Society of Digital Industry and Information Management*, Vol. 19, No. 1, pp. 31-42, March 2023. https://doi.org/10.17662/ksdim.2023.19.1.031

[6] J.-H. Heo, S.-H. Kwon, and Y.-S. Choi, “Vulnerability Analysis for an Next Generation IoT Infrastructure Authentication Protocol,” *Journal of Information Technology and Architecture*, Vol. 19, No. 4, pp. 263-273, December 2022. http://doi.org/10.22865/jita.2022.19.4.263

[7] J.-G. Kim and Y.-S. Choi, “Weakness of Blockchain-Based Electronic-Health Recording and Sharing Scheme,” *Journal of Digital Contents Society,* Vol. 22, No. 8, pp. 1281-1288, August 2021. http://dx.doi.org/10.9728/dcs.2021.22.8.1281

[8] Y. Choi, “Weaknesses and Improvement of User Authentication Scheme against Smart-Card Loss Attack,” *The Journal of the Institute of Internet, Broadcasting and Communication*, Vol. 16, No. 6, pp. 95-101, December 2016. https://doi.org/10.7236/JIIBC.2016.16.6.95

[9] A. Yamada and E. Lee, “Analysis of Research Trends in Homomorphic Encryption Using Bibliometric Analysis,” *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 33, No. 4, pp. 601-608, August 2023. https://doi.org/10.13089/JKIISC.2023.33.4.601

[10] Purnima, S. Sharma, and D. K. Verma, “LABE: Challenges and Perspectives of Attribute-Based Encryption in Lattice-Based Cryptography,” in *Proceedings of the 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, Gautam Buddha Nagar, India, pp. 1145-1151, December 2023. https://doi.org/10.1109/UPCON59197.2023.10434485

[11] J. Tan, Y. Sun, J. Gao, and H. Jung, “A Study on Secure Storage of Cloud Data Based on Blockchain,” *Journal of Digital Contents Society,* Vol. 25, No. 6, pp. 1581-1588, June 2024. https://doi.org/10.9728/dcs.2024.25.6.1581

[12] H. Shin and T. Shon, “Application and Comparative Analysis of Machine Learning-Based Cloud Digital Forensics,” *Journal of Digital Contents Society,* Vol. 25, No. 5, pp. 1301-1313, May 2024. https://doi.org/10.9728/dcs.2024.25.5.1301

[13] H.-W. Park and Y.-S. Choi, “Security Analysis of a Lightweight Mutual Authentication Protocol for V2V Communication in IoV,” *Journal of Digital Contents Society*, Vol. 23, No. 8, pp. 1509-1517, August 2022. https://doi.org/10.9728/dcs.2022.23.8.1509

[14] D.-E. Cho, “Smart Contract Security Vulnerability Analysis and Security Automation Model,” *Journal of Digital Contents Society*, Vol. 25, No. 4, pp. 1087-1094, April 2024. https://doi.org/10.9728/dcs.2024.25.4.1087

[15] B. W. Suh and J. Kim, “A Case Study of Korea’s Fractional Investment in Blockchain-based Digital Platforms,” *Journal of Digital Contents Society,* Vol. 24, No. 3, pp. 617-629, March 2023. https://doi.org/10.9728/dcs.2023.24.3.617

이정훈(Jung-Hun Lee)

2019년～현　재: 인제대학교 컴퓨터공학부 학사과정

※관심분야 : 정보보호(Information security), 디지털포렌식(Digital Forensic), 암호학(Cryptography) 등

최윤성(Youn-Sung Choi)

2006년 : 성균관대학교 정보통신공학부 학사

2007년 : 성균관대학교 전자전기컴퓨터공학부 석사

2015년 : 성균관대학교 전자전기컴퓨터공학부 박사

2016년～2020년: 호원대학교 사이버보안학과 조교수

2020년～현　재: 인제대학교 AI 융합대학 AI 소프트웨어학부 조교수

※관심분야 : 정보보호(Information security), 디지털포렌식(Digital Forensic), 산업보안(Industrial security) 등