Fog 기반 IoT 환경을 위한 상호 인증 및 키 합의 방식의 보안 취약점 분석 및 대응 방안

김태훈, 최지혜, 권덕규, 박영호

경북대학교

kimth028@knu.ac.kr, jihye@knu.ac.kr, kdk145@knu.ac.kr, parkyh@knu.ac.kr

Cryptanalysis and Countermeasures of Mutual Authentication and Key Agreement Scheme in Fog-Enabled IoT Environments

Kim Tae Hun, Choi Ji Hye, Kwon Deok Kyu, Park Young Ho

Kyungpook National Univ.

요 약

포그 컴퓨팅 기반 사물인터넷 환경에서 포그 서버를 이용하여 전송 지연을 낮추고 클라우드 서버에 걸리는 부하를 줄이고, 사용자에게 실시간 서비스를 제공할 수 있다. 그러나 이러한 무선 통신 환경은 가장 공격, 도청 공격, 메시지 가로채기 등 여러 보안 공격에 취약하기에 안전한 인증 프로토콜은 필수적이다. 2024년에 Harbi 등이 블록체인을 활용한 포그 기반 인증 프로토콜을 제안하였으나 내부자 공격, 검증자 도난 공격에 대해 취약함을 발견하였다. 또한 사용자에 대한 비추적성을 보장하지 않음을 확인하였다. 본 논문에서는 Harbi 등의 프로토콜을 분석하여 보안 취약점을 제시하고 안전한 상호 인증을 위한 대응 방안을 제시한다.

Ⅰ. 서 론

사물인터넷(IoT, Internet of Things)은 스마트 팩토리, 헬스케어 등 여러 분야에 활용되고 있다 [1]. 사물인터넷 기기들은 일반적으로 저장 공간의 크기가 작고 컴퓨팅 파워가 낮기 때문에 클라우드 서버에 연결되어 데이터를 업로드, 처리, 저장하게 된다 [2]. 그리고 사용자들은 인증 과정을 거쳐 클라우드 서버에 저장된 데이터에 접근할 수 있다. 예를 들어, IoHT(Internet of Health Things) 환경에서는 환자 몸에 부착된 센서들의 데이터가 서버로 전송되고, 의료진은 서버에 접속하여 환자의 생체 정보를 열람할 수 있다 [3]. 이처럼 IoT 환경은 사용자에게 편리한 서비스를 제공할 수 있지만, 하나의 클라우드 서버 중심의 통신 환경은 서버에 과도한 트래픽 부하가 걸릴 수 있다는 점과, 실시간 데이터 활용이 어렵다는 문제점들이 있다 [4]. 이 문제들을 해결하기 위해 포그 컴퓨팅 기술을 도입하였다. 여러 지역에 분산된 포그 노드를 활용해 클라우드 서버의 부담을 줄이고 사용자의 편의성을 증대시킬 수 있다 [5]. 그러나 이런 포그 노드의 도입으로 인해 보안 위험성이 증가하였기에, 포그 노드를 포함한 삼자 간의 상호 인증 프로토콜이 지속적으로 연구되고 있다. 특히 Harbi 등은 포그 노드들을 블록체인으로 연결하여 사용자 인증 과정의 신뢰성을 높였다 [6]. 그러나 Harbi 등이 제안한 프로토콜에서 내부자 공격, 검증자 도난 공격에 대한 취약성이 발견되었다. 또한, 사용자에 대한 비추적성이 보장되지 않는다. 이에 본 논문에서는 Harbi 등이 제안한 프로토콜이 여러 보안공격에 취약함을 보이고, 대응 방안을 제시한다.

Ⅱ. 본론

Harbi 등이 제안한 인증 및 키 합의 방식은 초기화 단계, 사용자 등록 단계, 인증 단계로 구성된다. 포그 노드와 클라우드 서버는 SA(System Administrator)에게 비밀 파라미터를 전송 받고, 사용자는 포그 노드에 등록 단계를 거친 후 상호 인증을 하게 된다. 본 논문에서 사용되는 시스템 모델은 그림1과 같다.

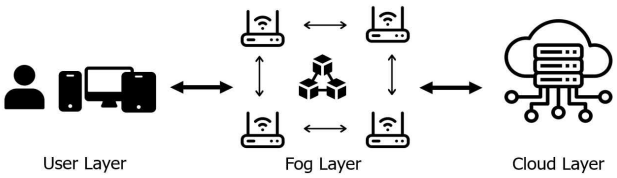

그림 1. 시스템 모델.

2.1 Harbi 등의 초기화 단계

그림 2는 Harbi 등이 제안한 인증 프로토콜의 초기화 단계이다.

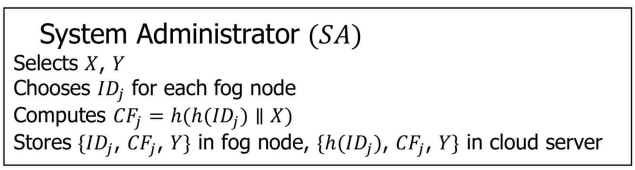

그림 2. 초기화 단계.

2.2 Harbi 등의 사용자 등록 단계

그림 3는 Harbi 등이 제안한 인증 프로토콜의 사용자 등록 단계이다.

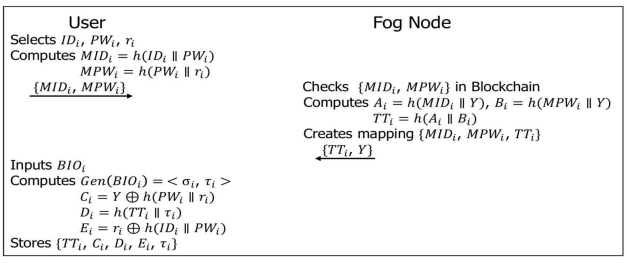

그림 3. 사용자 등록 단계.

2.3 Harbi 등의 인증 단계

그림 4는 Harbi 등이 제안한 인증 프로토콜의 인증 단계이다.

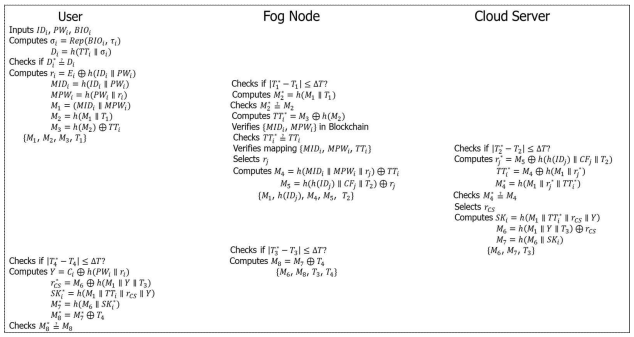

그림 4. 인증 단계.

2.4 보안 취약점

Harbi 등이 제안한 프로토콜은 내부자 공격, 검증자 도난 공격에 취약하고, 사용자의 비추적성을 보장하지 않는다.

2.4.1 내부자 공격

공격자는 정상적인 사용자처럼 등록과 인증 과정을 거친다. 이 과정에서 비밀 키 $Y = C_i \oplus h(PW_i \| r_i)$를 계산한다. 그 후 공격자는 다른 사용자의 세션에 침입해 $\{M_1, M_2, M_3, T_1\}$와 $\{M_6, M_7, T_3\}$를 탈취하여 $TT_i = M_3 \oplus h(M_2)$, $r_{CS} = M_6 \oplus h(M_1 \| Y \| T_3)$를 계산하여 세션 키 $SK_i = h(M_1 \| TT_i \| r_{CS} \| T_3)$를 계산해낼 수 있다.

2.4.2 검증자 도난 공격

공격자가 클라우드 서버에서 포그 노드를 검증할 때 필요한 비밀 값인 $\{h(ID_j), CF_j, Y\}$를 탈취한다고 가정한다. 그 후 공격자는 다른 사용자의 세션에서 $\{M_1, M_2, M_3, M_6, T_3\}$를 탈취하고 $TT_i = M_3 \oplus h(M_2)$, $r_{CS} = M_6 \oplus h(M_1 \| Y \| T_3)$를 계산하여 세션 키 $SK_i = h(M_1 \| TT_i \| r_{CS} \| T_3)$를 계산할 수 있다.

2.4.3 비추적성

사용자가 포그 노드에 보내는 메시지 $\{M_1, M_2, M_3, T_1\}$에서 $M_1 = (MID_i \| MPW_i)$이고, 각각 $MID_i = h(ID_i \| PW_i)$, $MPW_i = h(PW_i \| r_i)$로 계산된다. 그렇기에 사용자가 보내게 되는 M_1의 값은 동일하게 유지된다. 따라서, 공격자는 M_1의 값을 이용해 동일한 사용자를 추적할 수 있다.

2.5 취약점에 대한 대응 방안

Harbi 등이 제안한 인증 프로토콜은 3.1에서 증명된 바와 같이 내부자 공격과 검증자 도난 공격에 취약하고 비추적성을 보장하지 못한다. 이 문제점들은 해시 함수, 사전 공유 키와 난수를 적절하게 사용하지 못하여 발생하였다. 따라서 본 논문에서는 사전 공유 키와 해시 함수를 이용해 사용자 정보와 난수를 마스킹하고, 세션 키를 난수와 사용자 정보의 해시 값으로 계산하는 방안을 제시한다. 사용자 정보를 난수와 사전 공유 키로 마스킹을 하면 공격자의 추적을 방지할 수 있고, 사용자 정보가 포함된 세션 키를 계산하는 것을 불가능하게 할 수 있다.

Ⅳ. 결론

본 논문에서는 Harbi 등이 제안한 fog-enabled IoT 환경에서의 사용자, 포그 노드 및 클라우드 서버 간의 인증 프로토콜이 내부자 공격과 검증자 도난 공격에 취약하고 사용자에 대한 비추적성이 보장되지 않음을 증명하였다. 또한 위에 제시한 취약점을 해결하기 위해 난수와 사용자 정보 및 사전 공유 키를 활용하는 대응 방안도 제시 하였다. 본 논문에서 제시한 대응 방안을 이용하여 추후에 fog-enabled IoT 환경에 적합한 안전한 삼자간의 프로토콜을 제안할 것이다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00396797, Development of core technology for intelligent O-RAN security platform)

참 고 문 헌

[1] Sutrala, A. K., Obaidat, M. S., Saha, S., Das, A. K., Alazab, M., Park, Y. “Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems,” IEEE Transactions on Intelligent Transportation Systems, pp. 2316-2330, Feb. 2021.

[2] Park, K., Park, Y. “MIoT-CDPS: Complete decentralized privacy-preserving scheme for medical internet of things,” Internet of Things, 101250, Oct. 2024.

[3] Garg, N., Wazid, M., Das, A. K., Singh, D. P., Rodrigues, J. J., Park, Y. “BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment,” IEEE access, pp. 95956-95977, May. 2020.

[4] Kim, M., Yu, S., Lee, J., Park, Y., Park, Y. “Design of secure protocol for cloud-assisted electronic health record system using blockchain,” Sensors, pp. 2913-2933, May. 2020.

[5] Peter, N. “Fog computing and its real time applications,” Int. J. Emerg. Technol. Adv. Eng, pp. 266-269, Jun. 2015.

[6] Harbi, Y., Aliouat, Z., Harous, S., Gueroui, A. M. “Lightweight blockchain-based remote user authentication for fog-enabled IoT deployment,” Computer Communications, pp. 90-105. May. 2024.