IoT 시스템을 위한 상호인증 및 키 합의 방식의 보안 취약점 및 대응방안

김채언, 권덕규, 김명현, 박영호

경북대학교

chaeon@knu.ac.kr, kdk145@knu.ac.kr, kimmyeong123@knu.ac.kr, parkyh@knu.ac.kr

Cryptanalysis and Countermeasures of the Mutual Authentication and Key Agreement Scheme for IoT systems

Kim Chae Eon, Kwon Deok Kyu, Kim Myeong Hyun, Park Young Ho

Kyungpook National Univ.

요 약

임베디드 디바이스의 성능 및 통신 기술이 발전함에 따라 IoT(Internet of Things) 시장은 빠르게 성장할 것으로 예상된다. 기존 IoT 환경은 디바이스의 제한된 리소스 및 통신 지연의 문제가 있어 이를 극복하기 위한 다양한 연구가 이루어지고 있다. 포그 컴퓨팅 기술은 낮은 전송 지연, 클라우드 리소스 확장을 제공하여 기존 IoT의 한계를 극복할 수 있지만, 디바이스 캡처, 메세지 가로채기, 비밀 키 손상, 가장 공격 등의 보안 문제를 고려해야한다. 최근, Ali 등이 포그 컴퓨팅 기반 IoT 환경에서의 경량 익명 인증 및 키 합의 체계를 제안하였다. 하지만 임시 비밀 유출 공격, 검증자 도난 공격에 대한 보안 취약점을 발견하였고 서로간의 상호 인증이 보장되지 않았다. 본 논문에서는 보안 분석을 통해 Ali 등이 제안한 시스템의 보안 취약성을 입증하고 이를 개선할 대응 방안을 제시한다.

Ⅰ. 서 론

임베디드 디바이스의 성능 및 통신 기술의 발전으로 IoT(Internet of Things) 환경이 대두되고 있다. IoT 환경은 IoT 장치를 통해 수집한 데이터를 기반으로 분석 및 학습하여 더욱 적절하고 개별화된 맞춤형 서비스 제공이 가능하다. 이러한 IoT 시스템의 예로는 스마트 홈, 환경 실시간 모니터링, 의료 원격진료 등이 있다[1]. 최근에는 사람들의 다양한 서비스 요구에 따라, IoT의 각종 측정 기술과 발전된 데이터 통신 기술을 이용한 실시간 정보 및 개인 데이터 확보가 중요해지고 있다[2].

IoT 기기는 휴대성 및 편의성을 위해 상대적으로 연산능력과 저장공간에 한계가 있어, 이를 해결하기 위해 클라우드 기반의 효율적인 IoT 무선 통신 시스템에 대한 연구가 활발히 이루어지고 있다[3][4]. 반면, IoT 산업의 핵심인 데이터 활용을 위해서는 많은 양의 민감한 데이터 수집이 불가피하기에, 이로 인한 개인 프라이버시 침해 우려도 증가하고 있다. 빠르고 안정적인 데이터 통신뿐만 아니라 개인정보 보호를 위한 안전하고 신뢰할 수 있는 시스템 구축이 IoT 산업 발전의 핵심 요소이다[5].

최근 몇 년 동안 IoT 시스템의 개인정보 보호 및 보안 문제를 해결하기 위한 연구들이 제안되고 있다. Ali 등[6]은 포그 컴퓨팅 기반의 효율적인 통신 시스템을 적용해 IoT 환경에서의 안전하고 경량화된 익명 인증 및 키 합의 체계를 제안했다. 클라우드 서버 한 곳에만 데이터가 집중되는 트래픽 부하와 원거리로 인한 실시간 응답 서비스 지연의 문제점을 해결하기 위해, 데이터 발생 지점 주변에서 중간지점인 포그 서버를 만들어 선별적으로 데이터 분석 및 활용이 수행 가능한 시스템 모델을 제시했다. Ali 등은 이를 통해 효율적이고 빠른 통신 이점을 가지면서 보안성을 높인 상호 인증 및 키 합의 프로토콜을 제안하였다. 하지만 Ali 등이 제안한 프로토콜은 임시 비밀 유출 공격, 검증자 도난 공격에 취약하고 상호인증을 보장하지 않는다. 본 논문에서는 Ali 등이 제안한 IoT 환경에서의 인증 및 키 합의 방식의 취약점을 분석하고 이에 대한 적절한 대응 방안을 제시한다.

Ⅱ. 본론

2.1 시스템 모델

Ali 등이 제안한 시스템 모델은 그림 1.과 같다. 클라우드 계층, 포그 계층의 등록기관과 포그 서버 및 IoT 장치 계층으로 구성된다.

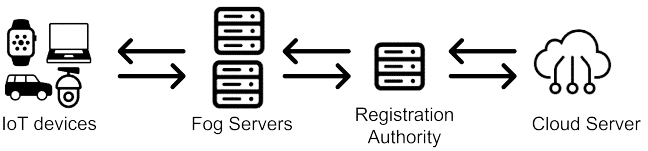

그림 1. Ali 등이 제안한 시스템 모델

- 클라우드 서버 (Cloud Server, CS) : 클라우드 서버는 최상위 계층인 클라우드 계층에 위치하며, 높은 컴퓨팅 능력과 저장 용량을 갖춘 데이터 센터이다. 클라우드 서버는 IoT 장치와는 물리적인 거리가 존재한다.
- 등록 기관 (Registration Authority, RA) : 등록기관은 IoT 및 포그 서버를 포그 계층에 안전하게 등록하는, 신뢰할 수 있는 제 3자이다. 등록기관은 포그 서버 근처에서 양호한 상태로 작동하고, 포그 서버와는 고속 링크로 연결되어 있어 통신 지연을 무시할 수 있다고 가정한다.
- 포그 서버 (Fog Server, FS) : 포그 서버는 물리적으로 클라우드 서버에 비해 IoT 기기와 가깝게 위치한 중간지점인 포그 계층에 위치한다. 등록센터에 자신을 등록하여 이후 안전한 통신을 위한 IoT와의 상호 인증을 진행한다. IoT에서 발생한 데이터를 1차적으로 모아 데이터 선별 및 분석을 어느정도 진행 후 최상위 계층인 클라우드 서버로 보낸다.
- IoT 장치 (IoT Device) : IoT 장치에는 차량, 스마트폰, 웨어러블 기기, 로봇 등 다양한 기기가 포함된다. IoT 장치는 포그 서버에 무선으로 연결되며, 수집한 다양한 정보를 보낸다. 안전하지 않은 무선 공개 채널 상에서 데이터를 주고 받기 때문에, 포그 서버와 IoT는 상호 인증 및 세션 키를 합의해야 한다.

2.3 프로토콜의 등록 단계

Ali 등이 제안한 프로토콜의 등록 단계는 그림 2., 그림 3.과 같다.

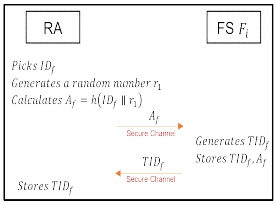

그림 2. 포그 서버 등록 단계

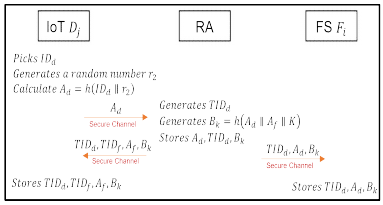

그림 3. IoT device 등록 단계

2.2 프로토콜의 인증 및 키 합의 단계

Ali 등이 제안한 프로토콜의 인증 및 키 합의 단계는 그림 3.과 같다.

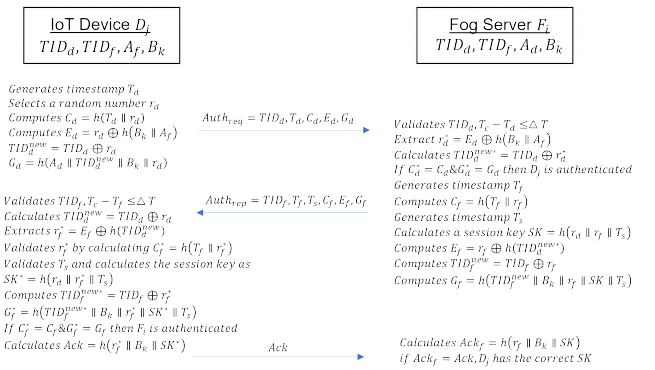

그림 4. Ali 등이 제안한 인증 및 키 합의 단계

2.3 보안 취약점

2.3.1 임시 비밀 유출 공격

세션 상의 특정 난수 r_d가 유출되었을 때, 공격자는 합법적인 IoT와 포그 서버의 비밀 값을 계산해낼 수 있다. 공격자는 공개 채널 상의 메시지에서 $\{TID_d, E_f, T_s\}$를 이용하여 세션 키 계산에 필요한 값 $\{r_d, r_f, T_s\}$를 구해낼 수 있다. 결론적으로 공격자는 알아낸 비밀값들을 통해서 세션 키 $SK = h(r_d \| r_f \| T_s)$를 알아낼 수 있으므로, Ali 등의 방식은 임시 비밀 유출 공격에 취약하다.

2.3.2 검증자 도난 공격

공격자는 등록과정에서 생성한 IoT와 포그 서버의 비밀값을 저장한 등록 서버를 공격할 수 있다. 이를 통해 얻어낸 비밀값$\{A_f, B_k\}$과 공개 채널 상의 메세지를 이용하여 얻어낸 $\{E_d, TID_d, E_f, T_s\}$ 값으로 세션 키 합의에 필요한 랜덤 난수 및 파라미터 값 $\{r_d, r_f, T_s\}$을 알아낼 수 있다. 이를 통해서 공격자는 세션 키를 계산해낼 수 있다. 따라서, 검증자 도난 공격에 취약하다.

2.3.3 상호 인증 특성

각 IoT와 포그 서버는 서로 인증하기 위해 검증 과정을 수행한다. 포그 서버는 $C_d = ? C_d^*$ 와 $G_d = ? G_d^*$, IoT 기기는 $C_f = ? C_f^*$, $G_f = ? G_f^*$ 확인을 통해 서로 검증하여 세션 키 합의를 진행한다. 모든 검증과정이 성공하면 마지막으로 Ack 메세지를 통해서 상호인증을 보장한다. 하지만 위에서 서술한 취약점으로 인해 인증 과정에 참여한 서로가 합법적인 참여자인지 제대로 인증하지 못한다. 위 보안 공격을 시도한 공격자는 획득한 비밀값을 이용하여 상호 인증 메세지를 위조 및 가장할 수 있다. 따라서, Ali 등이 제안한 프로토콜은 상호 인증을 보장할 수 없다.

2.4 대응 방안

Ali 등이 제안한 방식은 임시 비밀 유출 공격, 검증자 도난 공격에 취약한 문제점을 가지고 있다. 이러한 문제점은 세션 키 합의에 필요한 파라미터를 암호화하는 데에 비밀값이 부족하게 사용되었음에 있다. 본 논문에서는 비밀값과 생성한 난수를 해쉬 함수에 함께 사용하여 암호화의 보안성을 높이고 세션 키 SK의 암호화하는 방안을 제시한다. 또한 해쉬 함수와 XOR 연산만을 사용하여 계산 부하를 줄이고 효율성을 높여 IoT 환경에 적합한 경량화 암호 체계를 활용하는 방식을 제안한다.

Ⅲ. 결론

본 논문에서는 Ali 등이 제안한 포그 컴퓨팅 기반 IoT 환경에서의 인증 및 키 합의 방식의 보안 취약점을 분석하였다. 보안 분석을 통해 Ali 등이 제안한 방식이 임시 비밀 유출 공격, 검증자 도난 공격에 취약하고 상호 인증을 보장하지 않음을 입증하였다. 이러한 취약점을 개선하기 위해 비밀값, 난수와 해쉬함수를 혼합적으로 활용함으로써 기존의 효율성을 가지면서도 IoT 환경에 적합한 대응 방안을 제안하였다. 향후 제안한 방식을 실제 구현하여 IoT 환경에 알맞는 안전하고 효율적인 보안 체계를 설계할 예정이다. 또한 PUF(Physical Unclonable Function) 등 IoT 환경에 적용해 볼 수 있는 다양한 보안 인증 기술을 포함하여 안전하고 다양한 IoT 환경에 적용할 수 있는 프로토콜을 연구하고자 한다. 이후 비정형 및 BAN logic(Burrows-Abadi-Needham logic), ROR(Real-Or-Random) 모델을 이용하여 설계한 인증 방식의 안전성을 입증할 것이다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communicatio ns Technology Planning & Evaluation (IITP) grant funded by the Kor ea government(MSIT) (No.RS-2024-00396797, Development of core te chnology for intelligent O-RAN security platform)

참 고 문 헌

[1] Oh, J., Yu, S., Lee, J., Son, S., Kim, M., and Park, Y. “A secure and lightweight authentication protocol for IoT-based smart homes,” Sensors, pp. 1488-1502, Feb. 2021.

[2] Son, S., Park, Y., and Park, Y. “A secure, lightweight, and anonymous user authentication protocol for IoT environments,” Sustainability, pp. 9241-9262, Aug. 2021.

[3] Park, K., and Park, Y. “IAKA-CIOT: An improved authentication and key agreement scheme for cloud enabled internet of things using physical unclonable function,” Sensors, pp. 6264-6283, Aug. 2022.

[4] Oh, J., Lee, J., Kim, M., Park, Y., Park, K., and Noh, S. “A secure data sharing based on key aggregate searchable encryption in fog-enabled IoT environment,” IEEE Transactions on Network Science and Engineering, pp. 4468-4481, Dec. 2022.

[5] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., and Quwaider, M. “IoT Privacy and security: Challenges and solutions,” Applied Sciences, pp. 4102-4119, Jun. 2020.

[6] Ali, H., and Ahmed, I. “LAAKA: Lightweight anonymous authentication and key agreement scheme for secure fog-driven IoT systems,” Computers & Security, pp. 103770-103788, May 2024.