IoT 기반 스마트 파밍 환경을 위한 상호 인증 프로토콜의 보안 취약점 및 대응 방안

장현정, 최지혜, 손승환, 박영호

경북대학교

jungi1713@knu.ac.kr, jihye@knu.ac.kr, sonshawn@knu.ac.kr, parkyh@knu.ac.kr

Cryptanalysis and Countermeasures of the Mutual Authentication Protocol for IoT based Smart Farming Environments

Jang Hyeon Jung, Choi Ji Hye, Son Seung Hwan, Park Young Ho

Kyungpook National Univ.

요 약

사물 인터넷 (IoT), 인공 지능 (AI). 빅데이터 등의 기술 발전에 따라 이러한 기술들이 농업 분야에도 활발히 적용되고 있다. 대표적으로, 스마트 파밍 (Smart Farming) 은 다양한 센서와 디바이스를 활용해 농장 환경을 실시간으로 모니터링하고, 수집된 데이터를 기반으로 의사 결정을 수행하는 지능형 농업 방식이다. 이러한 환경에서는 센서와 디바이스 간 통신이 필수적이기 때문에, 안전한 데이터 전송과 상호 인증을 위한 경량 인증 프로토콜이 필요하다. 2024년 Rahaman 등은 스마트파밍 환경에서 센서와 디바이스, 서버 간 상호 인증 프로토콜을 제안하였다. 그러나 Rahaman 등이 제안한 프로토콜은 사칭 공격, 임시 키 유출 공격에 취약하며, 사용자의 불추적성을 보장하지 못한다. 본 논문에서는 비정형 분석을 통해 해당 프로토콜을 분석하고 안전한 상호 인증을 위한 대응 방안을 제시한다.

Ⅰ. 서 론

스마트 파밍 (Smart Farming) 은 전통적인 농업 방식에 사물 인터넷 (IoT), 인공 지능 (AI), 클라우드 컴퓨팅과 같은 첨단 기술을 적용하여 농업 생산량을 증대시키는 새로운 방식의 농업이다 [1]. AI와 IoT 기술이 통합된 스마트 파밍 환경은 주로 사용자, IoT 센서, 중앙 서버로 구성된다. IoT 센서는 주변의 온도, 습도 등 다양한 데이터를 실시간으로 수집하며 [2], 센서가 수집한 데이터는 중앙 서버로 전송되어 AI 분석의 기반이 된다. 중앙 서버는 데이터를 전처리하고, AI를 통해 이를 분석하여 작물별 생장 단계 및 수확 시기 등을 예측한다. 사용자는 주로 농부이며 AI 분석 결과를 전달받아 최종 농업 의사 결정을 효율적으로 수행할 수 있으며, 이를 통해 최소한의 자원으로 최대한의 농업 생산량을 달성할 수 있다. 이 과정에서 센서가 수집하는 데이터에는 사용자의 민감한 데이터가 포함된다[3]. 이러한 데이터들은 공개 채널을 통해 전송되기 때문에 도청, 위조, 재전송 등 다양한 보안 공격에 취약할 수 있어 데이터의 기밀성과 사용자 프라이버시 보호를 위한 상호 인증 프로토콜이 필요하다 [4].

2024년에 Rahaman 등은 AI와 IoT 기술이 통합된 스마트 팜 모니터링 환경을 위한 인증 프로토콜을 제안하였다 [5]. 본 논문에서는 Rahaman 등이 제안한 프로토콜에 대해 비정형 분석을 수행하고, 모바일 기기 도난 공격, 사칭 공격 등에 취약함을 확인하였다. 따라서 이를 보완하기 위한 보안성과 프라이버시를 강화할 수 있는 대응 방안을 제시한다.

Ⅱ. Rahaman 등이 제안한 상호 인증 방식

Rahaman 등이 제안한 인증 프로토콜은 사용자와 센서 등록 단계, 로그인 및 인증 단계로 구성된다. 사용자와 센서는 중앙 서버에 등록해야 하며, 등록 후 인증에 필요한 비밀 파라미터를 공유하게 된다. 그 후 인증 단계를 통해 사용자와 센서, 중앙 서버는 공통의 세션키를 공유할 수 있다.

2.1 Rahaman 등의 등록 단계

Rahaman 등이 제안한 프로토콜에서 사용자와 센서는 중앙 서버에 등록해야 한다. 등록 단계는 그림 1과 같다.

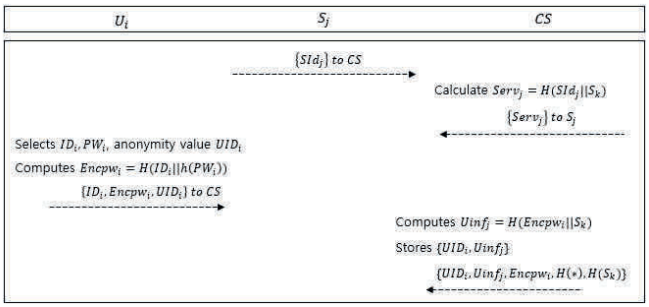

그림 1. 등록 단계.

2.2 Rahaman 등이 인증 단계

등록 단계에서 공유한 비밀 파라미터를 사용하여 사용자와 중앙 서버, 센서는 세션키를 합의한다. 인증 단계는 그림 2와 같다.

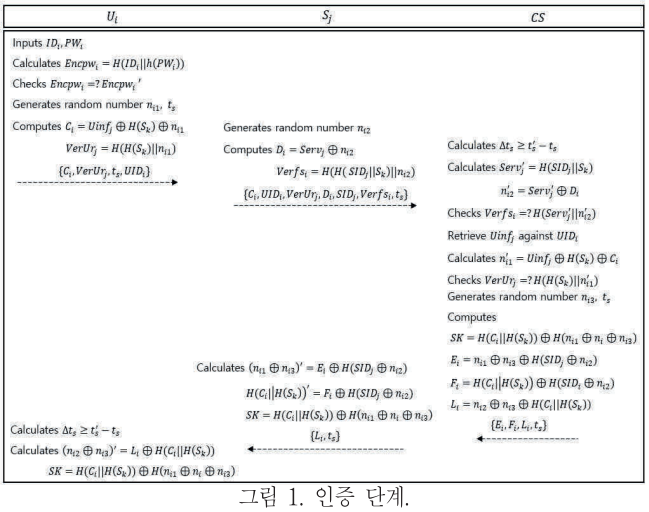

그림 1. 인증 단계.

2.3 Rahaman 등이 제안한 프로토콜의 보안 취약점

본 논문에서는 비정형 보안 분석을 통해 Rahaman 등이 제안한 인증 프로토콜의 취약점을 보인다. Rahaman 등이 제안한 프로토콜은 사용자 사칭 공격, 내부자 공격, 임시 키 유출 공격에 취약하고, 사용자의 추적 가능성을 보장하지 않음을 증명한다.

2.3.1 사용자 사칭 공격

공격자는 사용자의 모바일 기기를 탈취하여 power analysis attack을 통해 기기에 저장된 $\{UID_i, Uinf_i, Encpw, H(*), H(S_k)\}$를 획득한다. 공격자는 인증 요청 메시지를 만드는 데에 필요한 값인 $\{Uinf_i, H(S_k)\}$를 알게 되므로, 공격자의 난수 n_A와 타임스탬프 t_A를 생성하고, 인증 요청 메시지 $\{C_A, VerU_A, t_A, UID_i\}$를 생성하여 센서에게 전송할 수 있다. 인증 단계에서 센서와 중앙 서버는 공격자를 합법적인 사용자로 판단하고 인증을 진행하게 된다. 따라서 Rahaman 등의 프로토콜은 사용자 사칭 공격을 방어하지 못한다.

2.3.2 내부자 공격

공격자는 서버에 합법적인 사용자로 등록하여 인증을 수행할 수 있다고 가정한다. 등록 후 공격자는 중앙 서버 마스터키의 해시값 $H(S_k)$을 획득하게 된다. $H(S_k)$은 중앙 서버에 등록하는 모든 사용자가 공통으로 가지게 되므로, 공격자는 이 값을 활용하여 다른 사용자의 세션 키를 계산할 수 있다. 공격자는 공개 채널을 통해 전송되는 C_i를 가로채 $H(C_i||H(S_k))$를 계산할 수 있다. 그 후 UID_i, L_i를 통해 세 개의 난수 n_{i1}, n_{i2}, n_{i3}를 얻을 수 있고, 따라서 공격자는 다른 사용자가 공유하는 세션키 $SK = H(C_i||H(S_k)) \oplus H(n_{i1} \oplus n_{i2} \oplus n_{i3})$를 계산할 수 있다.

2.3.3 임시 키 유출 공격

세션 상의 임시 비밀 값인 세 개의 난수 $\{n_{i1}, n_{i2}, n_{i3}\}$가 유출된다면, 공격자는 세션키를 계산할 수 있다. 공격자는 중앙서버가 센서에게 전송하는 메시지인 $\{E_i, F_i, L_i, t_s\}$를 가로챈다. 공격자는 n_{i1}, n_{i3}, E_i를 통해 $H(SID_j \oplus n_{i2})$를 알아내고, 이 값과 F_i를 통해 $H(C_i||H(S_k))$를 알아낼 수 있다. 그 후 유출된 세 개의 난수와 알아낸 값을 통해 세션 키 $SK = H(C_i||H(S_k)) \oplus H(n_{i1} \oplus n_{i2} \oplus n_{i3})$를 계산할 수 있다.

2.3.4 사용자의 불추적성

Rahaman 등의 프로토콜에서 사용자는 임시 아이디인 UID_i를 사용한다. 이 임시 아이디는 인증 단계에서 공개 채널로 전송된다. 하지만 인증 단계에서 사용자의 임시 아이디를 업데이트하지 않기 때문에, 공격자는 사용자의 연속적인 인증을 추적할 수 있게 된다. 따라서 Rahaman 등의 프로토콜은 사용자의 불추적성을 보장하지 못한다.

2.4 대응 방안

Rahaman 등이 제안한 프로토콜은 사용자 사칭 공격, 내부자 공격, 임시 키 누출 공격에 취약하며 사용자 불추적성을 보장하지 않는다. Rahaman 등의 프로토콜에서는 사용자의 모바일 기기가 도난당할 경우 공격자가 사용자를 사칭할 수 있을 뿐만 아니라 세션 키를 계산할 수 있게 된다. 이는 사용자가 인증에 필요한 파라미터를 저장하는 데에 사용한 비밀 값이 부족했음을 나타낸다. 따라서 등록 단계에서 사용자는 난수를 생성하여 해시 함수를 사용함으로써 인증 파라미터의 보안성을 높일 필요가 있다. 또한 세션 키를 계산할 때 사용되는 SID_j, C_i 는 공개 채널을 통해 얻을 수 있는 값이다. 따라서 세션 키를 사용할 때 공개 채널로 전송되는 값의 사용을 줄이고, 센서와 사용자만이 알 수 있는 값으로 계산한다. 사용자의 불추적성을 보장하기 위해, 인증 단계의 마지막에 사용자의 임시 아이디를 업데이트하는 과정 또한 필요하다.

Ⅲ. 결론

본 논문에서는 Rahaman 등이 제안한 스마트 파밍 환경에서 사용자, 센서, 중앙 서버 간의 인증 프로토콜을 분석하였다. 보안 분석을 통해 Rahaman 등이 프로토콜이 사용자 사칭 공격, 임시 키 유출 공격에 취약하고, 사용자 불추적성을 보장하지 못한다는 것을 입증하였다. 이러한 취약점을 보완하기 위해 난수와 해시값을 사용해 사전에 공유한 파라미터를 안전하게 저장함으로써 세션 키의 보안성을 높일 수 있었다. 본 논문에서 제시한 대응 방안을 통해 IoT 기반 스마트 파밍 환경에서 사용자와 센서 간의 세션 키 공유를 위한 구체적인 인증 프로토콜을 제안할 수 있다.

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 t echnology for intelligent O-RAN security platform)

참 고 문 헌

[1] Farooq, M. S., Riaz, S., Abid, A., Abid, K., and Naeem, M. A. “A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming,” Ieee Access, pp. 156237-156271. Oct. 2019

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

[3] Yu, S., Jho, N., and Park, Y. “Lightweight three-factor-based privacy-preserving authentication scheme for iot-enabled smart home,”. IEEE Access, pp. 126186-126197. Sep. 2021

[4] Kwon, D. K., Yu, S. J., Lee, J. Y., Son, S. H., and Park, Y. H. “WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor network,“. Sensors, pp. 936. Jan. 2021

[5] Rahaman, M., Lin, C. Y., Pappachan, P., Gupta, B. B., and Hsu, C. H. “Privacy-centric AI and IoT solutions for smart rural farm monitoring and contro,“. Sensors, pp. 4157. Jun. 2024