African Journal of Applied Research
Special Issue: Artificial Intelligence and Engineering: Emerging Technologies and Applications
Vol. 12, No. 6 (2026), pp. 400-432
http://www.ajaronline.com
Received January 1, 2026
Peer reviewed: April 25, 2026
Revised: August 15, 2026
Published: September 2026

ULTRA-LIGHTWEIGHT KEY AGREEMENT FOR SECURE ELECTRONIC HEALTH RECORDS IN THE INTERNET OF HEALTHCARE THINGS

Salih Abdulridha, M.[1], Al Chaab, W.[2], and Hassan Adday, G.[3]
[1]*Department of Computer Information Systems, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq.*
[2]*Department of Mathematics, College of Science, University of Basrah, Basrah, Iraq.*
[3]*Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq.*
[1]*maha.abdulradha@uobasrah.edu.iq*
[2]*wafaa.khudhair@uobasrah.edu.iq*
[3]*ghaihab.aday@uobasrah.edu.iq*

ABSTRACT

Purpose: The purpose of this study is to develop an ultra-lightweight mutual authentication and key agreement protocol for securing Electronic Health Records (EHRs) in Internet of Healthcare Things (IoHT) environments.

Design/Methodology/Approach: The proposed protocol employs lightweight cryptographic primitives, specifically SHA-256 hash functions and bitwise XOR operations, to eliminate computationally expensive public-key cryptography and fuzzy-extractor operations at the user-node level. Local biometric authentication and fresh random nonces are incorporated to enhance user identity privacy and provide resistance against replay and DoS attacks, where confidentiality and integrity are enforced by cryptographically binding these parameters into the session transcript. The security of the protocol was formally verified using Burrows–Abadi–Needham (BAN) logic with explicitly defined message idealisations and automated simulation through ProVerif. Finally, the protocol's performance was evaluated and compared with existing schemes by itemising computational and communication costs under a unified benchmarking platform and energy model**.**

Research Limitation: The proposed protocol is primarily designed for resource-constrained IoHT environments and relies on lightweight cryptographic primitives. Therefore, its applicability may be limited in environments requiring more computationally intensive cryptographic mechanisms or hardware-dependent security primitives.

Findings: The security analysis demonstrates that the proposed protocol provides mutual authentication and session key secrecy while resisting spoofing, impersonation, replay, cloning, MITM, and DoS attacks. Performance evaluation shows an execution time of 0.0225 ms, a communication cost of 1344 bits, and an energy consumption of only 1.1138 μJ.

ISSN: 2408-7920
Copyright ⓒ African Journal of Applied Research
Arca Academic