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

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

Compared with existing approaches, the proposed protocol achieves up to a 74.2% reduction in computational overhead.
Practical Implication: Its low execution time, communication cost, and energy consumption make it suitable for practical deployment in secure EHR management and other resource-constrained healthcare applications.
Social Implication: By improving the security and privacy of health information while reducing authentication resource requirements, the proposed protocol can support safer, more reliable digital healthcare services.
Originality/Value: This study introduces an ultra-lightweight mutual authentication and key agreement protocol that combines hash functions, XOR operations, local biometric authentication, and fresh random nonces without relying on computationally expensive asymmetric cryptography or hardware-dependent Physical Unclonable Functions (PUFs).

Keywords: *Biometric. cyber-attacks. healthcare. lightweight cryptography. mutual authentication*

INTRODUCTION

The digital world has seen major developments in communications, networks, and data processing, leading to Internet of Things (IoT) systems that rely on data automation and secure cloud management (Khade et al., 2025). Given the importance of medical data and the need to secure and manage it, the IoT has been integrated with medical systems, giving rise to the Internet of Healthcare Things (IoHT) (Ketu & Mishra, 2021). Furthermore, it enables continuous patient tracking, real-time clinical monitoring, and effective mitigation strategies during global pandemics(Elhoseny et al., 2018). Concurrently, the processing of telemetry data within IoHT environments empowers healthcare providers to deliver proactive services, thereby accelerating diagnostic timelines and ensuring immediate therapeutic interventions, (Khan et al., 2025; Elhoseny et al., 2018).

Essentially, authentication is crucial for securing IoHT systems. It is used to control access and permissions based on user identity, role and personal information (Sahu et al., 2022), and serves as the primary shield against cyber-attacks such as replay attacks, spoofing, Denial of Service (DoS) attacks, and Man-in-the-Middle (MITM) attacks (Ray et al., 2021; Hussien et al., 2016).

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

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

In IoHT, Authentication protocols vary based on the included factors, such as the server, used encryption methods, user types and roles, protocol weight, and the number and type of authentication factors (Abuhamad et al., 2021).

Developers often focus on external attacks, but internal threats from user compromises are also significant. Password-based authentication, though convenient, is vulnerable to offline guessing attacks. Therefore, more robust and secure systems have been proposed, including mutual authentication, multi-factor authentication, and biometrics (Qiu et al., 2019)using QR codes, digital certificates and tokens, which are crucial to secure smart healthcare system communication (Almadani et al., 2023; Ding & Xie, 2023 ;Devi et al., 2022). Furthermore, Quick Response (QR) codes improve user access by reducing errors and complexity associated with manual input, thereby strengthening authentication efficiency in IoHT environments. Furthermore, the combination of a digital signature and cryptography in IoHT provides robust resistance against tampering, forgery, and MITM attacks (Alzaidi et al., 2024).

Implementing biometric features adds robustness and security by leveraging unique human characteristics such as face, fingerprint, or even palm, guaranteeing user uniqueness and providing non-repudiation across IoHT networks(Villegas-Ch & García-Ortiz, 2023). To secure the transmission of these biometric templates and maintain data integrity, lightweight cryptographic primitives, most notably the SHA-256 hashing algorithm, are deployed to build robust barriers against brute-force and collision attacks.

Moreover, Elliptic Curve Cryptography (ECC) is a leading approach for asymmetric key management, offering public-key security comparable to traditional RSA but with significantly smaller key sizes (Almadani et al., 2023). This mathematical efficiency mainly reduces computational latency and memory consumption, thereby optimising energy preservation for resource-constrained IoHT nodes. Despite these advantages, embedding these cryptographic mechanisms into practical healthcare infrastructures remains bounded by critical open challenges. The high communication cost and computational complexity of cryptographic operations during authentication and active sessions consume more resources and drain the battery life of wearable medical sensors. Interoperability is another challenge when operating heterogeneous IoHT ecosystems, where real-time patient monitoring demands near-zero latency that standard cryptographic architectures often fail to sustain (Akilan et al., 2024).

ISSN: 2408-7920
Copyright Ⓒ African Journal of Applied Research

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

RELATED WORK

In healthcare systems, the most common user-friendly authentication method is traditional password-based authentication; however, due to its simplicity, it is insufficient to secure sensitive IOHT data against various cyber threats. These systems are vulnerable to compromise if credentials are exposed, shared or stolen. To enhance security and data integrity, multi-factor authentication (MFA), including 2FA and 3FA, with robust cryptographic techniques has been proposed as a countermeasure to these inherent threats.

In 2022, Shukla and Patel (Shukla & Patel, 2022) developed a multi-factor authentication protocol to mitigate vulnerabilities found in a previous protocol (Chen & Chen, 2021). This protocol used ECC for cloud computing and successfully mitigated attacks like replay attacks, KSSTI, user impersonation attacks, spoofing attacks, password-guessing attacks, and privileged insider attacks. However, their protocol is vulnerable to replay, user linkability, and DoS attacks (Adel Yaseen et al., 2025).

In 2023, Yadav et al. presented a lightweight dual-factor authentication protocol. This protocol was designed to inherit the robustness of Extensible Authentication Protocol (EAP) encryption algorithms while integrating lightweight cryptographic primitives for enhancing data security, such as random nonces, Hash, and symmetric and asymmetric key cryptography (Yadav et al., 2023); however, it is prone to DDoS attacks.

Kim et al. (2023) developed an enhanced lightweight user authentication scheme for the IoMT, leveraging Hash and XOR for ensuring privacy. Their scheme demonstrated security against known cyber-attacks and improved performance by up to 250 % (Kim et al., 2023). However, the protocol's sequential calculations are vulnerable to DoS attacks, as attackers can overwhelm the system with requests, forcing computations before detection.

Another robust authentication scheme was proposed by Abbasi et al. (2024) using a fuzzy extractor, XOR and the ECC method for building a lightweight protocol to secure a cloud-based e-healthcare system (Abbasi et al., 2024). Still, it lacks a scalability analysis and is prone to a traceability attack (Alzahrani & Alzahrani, 2025).

ISSN: 2408-7920
Copyright Ⓒ African Journal of Applied Research

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

To address the complexity and cost challenges in authentication protocols, Kook et al. (2024) presented a one-way hash-based lightweight protocol. The protocol ensures secure communication through message authentication and a dynamic encryption key per transmission. The system security was analysed and proved to be resilient against current attacks, while performance analysis showed a 105% improvement in computational efficiency over prior protocols (Kook et al., 2024). However, it is vulnerable to DoS attacks and has deficient traceability.

Wang & Han, (2025) introduced a WSN privacy scheme used PUF chaotic map cryptography, employing one-time pseudonyms and dynamic credentials. This method uses biometric features, SHA-256, and XOR operations to resist cyber threats in WSNs, providing anonymity and session-key confidentiality and ensuring untraceability and forward secrecy. It reduces communication and computational overhead while enhancing security, though it still poses scalability and decentralisation issues. Abdul-Aziz et al. (2025) proposed another authentication protocol for WBANs that combines biometrics and asymmetric-key cryptography to ensure session-key secrecy and reliability against forgery and insider attacks. However, their protocol was vulnerable to replay and sensor node impersonation attacks during authentication. This vulnerability arises from the absence of timestamps and fresh nonces in request messages, allowing attackers to reuse intercepted messages for illegitimate access or to launch DoS attacks.

For privacy preservation, Alzahrani and Alzahrani (2025) introduced an authentication protocol utilising the ECC cryptographic algorithm, XOR operation and SHA-256. For robustness verification, the RoR model and ProVerif were used; the performance evaluation covered computational demands, communication overhead, and storage requirements. The protocol demonstrates significant improvements over previous methods: 93% in computation enhancement, 53% in communication and 62% in energy saving, making it ideal for e-healthcare systems (Alzahrani & Alzahrani, 2025). Kulikov (2025) presented a new XOR-based secret-sharing scheme that prioritised simplicity and efficiency but did not propose an authentication scheme. It emphasises a (3,2) threshold secret-sharing algorithm that is practical for systems with constrained computational resources. Yet, it has not been tested within a protocol or system (Kulikov, 2025).

A recent study by Jang et al. (2026) introduced a lightweight and highly robust authentication scheme for resource-constrained environments. This proposed scheme relied on XOR and hash functions, and Ascon cryptography was integrated for data integrity and cost reduction (Jang et al., 2026). However,

ISSN: 2408-7920
Copyright Ⓒ African Journal of Applied Research

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

their scheme is vulnerable to DoS attacks during authentication. This vulnerability arises because the Multi-Gateway (MGW) processes every incoming request without pre-verifying user legitimacy, allowing attackers to flood the MS with requests containing fake ID_u and $r1$, that exhaust the MGW's resources.

Lim et al.(2026) presented a MioT environment authentication protocol based on hash functions, XOR operations, and PUFs. The proposed protocol proved resilient to stolen verifiers, eavesdropping, ephemeral secret leakage, and failed untraceability, offering a robust, privacy-preserving solution for MioT (Lim et al., 2026). Still vulnerable to insider attacks and offline password guessing. Almagrabi (2026) proposed an authentication protocol utilising the discrete logarithm problem (DLP) and SHA-2. This protocol aims to secure smart home remote surveillance by mitigating impersonation, password-guessing attacks, and privacy concerns arising from weak cryptographic designs (Almagrabi, 2026). However, it has several weaknesses, including vulnerabilities in generating, sharing, and deriving both public and private keys. Additionally, it lacks resilience against DoS attacks and incurs high computational costs. Table(1) contains a comparison of authentication protocols mentioned in this section.

Table 1: Comparison of related works

Reference	Year	Technology	Contributions	Limitations
Shukla and Patel (Shukla & Patel, 2022)	2022	ECC, Biometrics	Mitigate replay attacks, KSSTI, user impersonation attacks, spoofing attacks, password-guessing attacks, and privileged insider	Vulnerable to user linkability, replay, and DOS attacks
Yadav et al (Yadav et al., 2023)	2023	EAP encryption, Hash functions, and symmetric and public-key cryptography	Lightweight, cyber-attacks mitigation	Exposure to DDOS attacks
Abbasi et al. (Abbasi	2024	Fuzzy extractor, XOR and the ECC	Lightweight, mutual authentication; anonymity and withstanding replay attacks	Susceptibility to a traceability attack and

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

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

et al., 2024)				scalability issues
Kook S. Et al (Kook et al., 2024)	2024	Hash function, MAC	Resilience against well-known attacks	No traceability and vulnerable to DOS attacks.
Wang & Han (Wang & Han, 2025)	2025	PUF-based chaotic map cryptography , biometric features, SHA-256 and XOR	Providing session key confidentiality, forward secrecy, ensuring anonymity and untraceability	Issues of scalability and decentralizatio n
Abdul-Aziz et al. (Abdul-Aziz Mutlaq et al., 2025)	2025	Biometrics and asymmetric cryptography	Ensure session key secrecy and reliability against forgery and insider attacks	Susceptible to replay attacks, sensor node impersonation during authentication and DOS attacks
Alzahrani and Alzahrani (Alzahrani & Alzahrani, 2025)	2025	ECC, SHA-256, and XOR	62% less energy, 53% less communication, 93% less computation	Vulnerable to spoofing and eavesdropping attacks
Jang et al. (Jang et al., 2026)	2026	Ascon, XOR and Hash functions	Data integrity and cost reduction	Vulnerable to DOS attacks

ISSN: 2408-7920
Copyright Ⓒ African Journal of Applied Research

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

Lim et al. (Lim et al., 2026)	2026	XOR, Hash, and PUF	Resilient to eavesdropping, stolen verifier, ephemeral secret leakage attacks and ensures privacy-preserving	Vulnerable to insider attacks and offline password guessing attacks
Almagrabi (Almagrabi, 2026)	2026	Discrete logarithm problem (DLP) and SHA-2	Mitigating impersonation, password-guessing attacks, and privacy concerns arising from weak cryptographic designs	Issues in sharing and derivation of both public and private keys, vulnerable to DOS attacks

Primitive Tools

A. *Hash function (SHA-256)*

SHA-256, a cryptographic hash function developed by the NSA, generates a unique 256-bit (32-byte) hash from any input data (Martino & Cilardo, 2020). Its sensitivity to input changes, irreversibility, and collision resistance make it ideal for integrity, verification, and digital signatures. It's widely used in SSL, SSH, and blockchain. The SHA-256 process involves padding messages to a fixed size, dividing them into 512-bit blocks, and processing them through 64 rounds of logical functions and constants to produce the final 256-bit hash (Secure Hash Standard, 1995), (Jawad et al., 2024). Part of the SHA-2 family (which also includes SHA-1 and SHA-512), SHA-256 effectively resists brute-force and collision attacks, even on resource-constrained IoT devices (Issad et al., 2024). It offers a strong security upgrade from SHA-1 while avoiding the computational overhead of SHA-512 on 32-bit hardware, making it optimal for medical sensors (Dang, 2012).

B. *One-Time Password (OTP):*

It is a numeric or alphanumeric security code (usually 4 to 6 digits) that is automatically generated and has a very temporary validity (often ranging from 30 seconds to a few minutes). It is used only once to confirm a user's identity during login or to complete a financial transaction. The

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

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

OTP is considered a fundamental element of two-factor authentication (2FA) (Imamah, 2018). Even if a hacker succeeded in obtaining a password, they will not be able to access the account unless they possess the dynamic OTP code sent to the user's device. It is usually sent via SMS, which is the most common method, to the user's registered phone number or email address. Sometimes, it is sent using authenticator applications such as Google Authenticator or Microsoft Authenticator, which use algorithms that automatically generate codes every 30 seconds without requiring an internet connection. The OTP relies on two well-known algorithms developed by the IETF (Internet Engineering Task Force). First, HOTP (HMAC-based OTP): Relies on a digital counter; the OTP changes each time a new one is requested. Second: TOTP (Time-based OTP): Relies on a hash function that combines a shared secret key with the current device time, which explains why the key changes automatically every 30 seconds. OTP provides enhanced security with minimal computational overhead (Jonghoon Lee, 2013).

C. Biometric Information

For more robustness in an IoHT system, a second factor is usually added, such as Biometric measures, which will raise the authentication level and enforce access control policies(Abhishek & Yogi, 2015). he most popular biometric is fingerprint. It's easy to implement, reliable and unique. Fingerprint characteristics are categorized into three levels, each adding a different security level and accuracy to the system. Level 1 identifies based on ridge patterns, Level 2 on minutiae points, and Level 3 on microscopic features like sweat pores, ridges, and scars(Abood et al., 2026). While Levels 1 and 2 are used for basic pattern matching and general classification, Level 3 is crucial for accurate identification and forensic analysis, significantly reducing errors (specifically addressing both false acceptance and false rejection rates)(Cheon et al., 2014). Given the sensitivity of healthcare data, the proposed protocol incorporates Level 3 fingerprint authentication as a second factor for more reliability and authenticity.

RESEARCH METHODOLOGY

Research design. This study follows a protocol-design and analytical evaluation approach for an ultra-lightweight mutual authentication and session key agreement scheme in Internet of Healthcare Things (IoHT) environments. The workflow comprises protocol construction, verification of specified security properties, and comparative performance evaluation.

ISSN: 2408-7920
Copyright Ⓒ African Journal of Applied Research

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

Protocol construction. The architecture includes a user device (patient or healthcare professional) and a Hospital Server (HS). The protocol uses SHA-256 hashing, XOR masking, local Level 3 fingerprint verification, timestamps, and fresh nonces. Its setup, registration, and authentication/key-agreement stages are detailed below, together with the messages exchanged and the server-side role assignment.

Security evaluation procedure. Informal arguments examine the intended security properties and threats. BAN logic is used to reason about mutual authentication and the parties' beliefs concerning the negotiated session key. ProVerif is used under a symbolic Dolev–Yao attacker model to check session-key secrecy and injective authentication correspondences. These methods assess the stated model and assumptions, not every implementation-level attack.

Performance evaluation procedure. Computational cost is estimated from operation counts and benchmark execution times obtained using Python on a 13th-generation Intel Core i7 (2.40 GHz) computer with 16 GB RAM. Communication cost is computed by summing transmitted field sizes; energy is estimated from assumed voltage (3.3 V), current (15 mA), and execution time. The same analytical cost framework is applied to the six reported comparison schemes. The document does not specify trial counts, dispersion statistics, or measurements on IoHT hardware.

Proposed Protocol

A lightweight, robust protocol was designed to secure patient data from password-guessing attacks and maintain confidentiality. The proposed protocol was a two-factor authentication designed based on a level 3 fingerprint and password. It uses lightweight XOR and hash functions to ensure security while minimizing resource consumption in resource-constrained environments.

This improved architecture can be adopted as a unified basis for registering both patients and doctors as users within the system, since both possess the same basic verification elements: (username, password, and biometric fingerprint). However, to ensure the protocol is accurate, practical, and ready for implementation in a smart healthcare system, we added a crucial feature to differentiate between them during registration: a role indicator R_i. This allows the server to determine the type of file it will create in the database. If the user is a patient, it creates an Electronic Health Record (EHR); if the user is a doctor, it creates an Electronic Staff (ESR) record

ISSN: 2408-7920
Copyright Ⓒ African Journal of Applied Research

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

and Access Permits. Table(2) Contains the notations and the symbols used in writing and representing the protocol.

Table 2: List of notations used in the proposed protocol

Notation / symbols	Notation Description
HS	Hospital Server
U_i	User i
UP_i	User username
PW_i	User password
$h(.)$	One-way Hash
Kp	Secret key
$Fing_i$	Fingerprint information
UWP_i	Hashed password
T_1	Timestamps
$\oplus$	XOR
$\|$	Concatenate
r_i, S_i, a_1, a_2	Nonces
SK	Session key
R_i	User role (patient / doctor)
OTP	One time password

The protocol is consists of several phases:

A. Setup Phase:

The setup phase is the proactive step preceding registration and identity verification, during which the system generates, prepares and chooses the parameters and functions required by the protocol. Based on the modified and improved protocol, the configuration phase is divided into two parts: configuring the hospital server (HS) and configuring user devices (doctors and patients):

- HS setup: The HS selects security parameters and generates master secrets before accepting any user. This includes generating a highly random system master key (Kp) and storing it in a highly secure storage unit which never leaves the server. A secure hash function (h(·)) that complies with IETF standards (lightweight SHA-256 or SHA-3) is also selected. The user database is

ISSN: 2408-7920
Copyright Ⓒ African Journal of Applied Research

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

then configured, containing fields for variable pseudonyms (PID_is), generating a random numeric nonce value (S_i) for each user, and other registration values.

- User Device setup: involves setting up the system application (whether on the patient's phone or the doctor's computer/device at the hospital), which contains the bioprocessing function (LVL3_Bio) and checking the device's integrity to ensure that the working environment is secure (e.g., the phone is not rooted or jailbroken) to ensure that data cannot be extracted locally.

B. User Registration Phase:

The healthcare system requires users to register and authenticate for role-based access. This subsection will focus on the registration process for the two main user types: patients and doctors. the steps of the registration as follows:

1. The user Ui enters his personal information (Name, Birth, Phone,…) and chooses username UP_i, password PW_i and enter his fingerprint $Fing_i$ and role R_i. The Ui's device calculates $UFP_i = LVL3_Bio(Fing_i)$ and checks UFP_i locally; if mismatched: terminate, otherwise: computes $UWP_i = H(UP_i \parallel UFP_i)$ then $Select\ T_1$ as timestamp and $r_i \in Z^*$, calculates $UID_i = H(UP_i \parallel r_i)$, then forms the registration's request $M1 = (UP_i, UWP_i, UID_i, R_i, T_1)$ and sends it to the HS.
2. When the HS receives M1, first: it checks the time freshness, then generates an OTP and sends it to the Ui phone number; if the OTP is unconfirmed, then terminate; otherwise: checking the user role R_i wither 'P' →initiates an EHR for Patient or else 'D' → ESR for Doctor.
3. The HS generates $S_i \in Z^*$ and computes $SIP_i = h(UP_i \parallel UWP_i \parallel Kp \parallel S_i)$, $SWP_i = h(UWP_i \parallel Kp) \oplus S_i$ and $save\{SIP_i, SWP_i, S_i\}$; finally constructs replay message $M2 = \{SIP_i, S_i, T_2\}$ and sends it to the U_i.
4. Upon receiving M2, the U_i selects a timestamp to verify the message's validity, computes $NU_i = h(UP_i \parallel UWP_i \parallel S_i)$, $MU_i = NU_i \oplus SIP_i$ and save the login parameters $\{MU_i, S_i\}$ in his personal device. As in figure (1).

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

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

U_i	HS
$Enter\ user's\ personal\ information$ $Enter\ UP_i, PW_i, Fing_i, R_i$ $UFP_i = LVL3_Bio(Fing_i)$ $If\ not\ UFP_i\ then\ terminate$ $Else$: $UWP_i = H(UP_i \parallel UFP_i)$ $Select\ T_1$ as timestamp and $r_i \in Z^*$ $UID_i = H(UP_i \parallel r_i)$ $M1 = (UP_i, UWP_i, UID_i, R_i, T_1)$	
	$Selest\ T_2$ $check\ \lvert T_2 - T_1\rvert < \triangle T$ $Generate\ OTP$ $Send\ OTP\ to\ U_i$ $If\ \ OTP\ not\ confirmed\ then\ terminate$ $Else$: $If\ R_i =' P'\ then: Initiate\ EHR$ $Else: Initiate\ ESR$ $Generate\ S_i \in Z^*$ $SIP_i = h(UP_i \parallel UWP_i \parallel Kp \parallel S_i)$ $SWP_i = h(UWP_i \parallel Kp) \oplus S_i$ $save\ \{SIP_i, SWP_i, S_i\}$ $M2 = \{SIP_i, S_i, T_2\}$
$Selest\ T_3$ $check\ \lvert T_3 - T_2\rvert < \triangle T$ $\mathrm{NU}_i = h(UP_i \parallel UWP_i \parallel S_i)$ $MU_i = NU_i \oplus SIP_i$ $SAVE\ \{\mathrm{MU}_i, S_i\}$	

Figure1: Registration phase

C. *Authentication phase:*

The login and authentication phase involves mutual authentication between users (patients/doctors) and the Healthcare Server (HS). Secret keys are established with the HS as an intermediary. The design of the login and authentication phase relies on using data stored locally on the user's device and secrets stored on the HS to verify mutual identity without transmitting any secrets over the network. The detailed points below show this phase:

1. The U_i enters his $UP_i, PW_i, Fing_i\ and\ R_i$, the local detection for the fingerprint is performed, if the $Fing_i$ is confirmed then U_i's application computes $UWP_i = h(UP_i \parallel UFP_i)$, $select\ T_1$ as a timestamp $and\ nonce\ a_1 \in Z^*$, the user application computes $\mathrm{NU}_i = h(UP_i \parallel UWP_i \parallel S_i), SIP_i =$

Copyright Ⓒ African Journal of Applied Research
Arca Academic

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

$NU_i \oplus MU_i$, $UID_i = h(UP_i \parallel a_1)$ and $A_1 = h(\text{SIP}_i \parallel UID_i \parallel a_1 \parallel T_1)$. Then it forms the login message M1= $\{A_1, UID_i, a_1, T_1\}$ and forwards it to the HS.

2. After M1 reception, The HS selects T_2 and does checking $|T_2 - T_1| < \triangle T$, if the time is fresh then: the HS retrieves the stored SIP_i related to the U_i to compute $A_1^* = h(\text{SIP}_i \parallel UID_i \parallel a_1 \parallel T_1)$ and checks $if\ A_1^* \stackrel{?}{\neq} A_1\ then$ terminate; else $select\ a_2 \in Z^*$, computes $SK_i = h(\text{SIP}_i \parallel a_1 \parallel a_2)$ and $A_2 = h(SK_i \parallel a_2 \parallel T_2)$. Finally, The HS constructs replay message M2=$\{A_2, a_2, T_2\}$ and sends it to the U_i.
3. For mutually authenticated, The U_i receives M2 and checks the time freshness, then computes the check values: $SK_i^* = h(\text{SIP}_i \parallel a_1 \parallel a_2)$ and $A_2^* = h(SK_i^* \parallel a_2 \parallel T_2)$, performs the operation $(if\ A_2^* \stackrel{?}{\neq} A_2)$, if true then terminate, otherwise : user is authenticated and the key is established. As illustrated in figure(2).

U_i	HS
$Enter\ UP_i, PW_i, Fing_i, R_i$ $UFP_i = LVL3_Bio(Fing_i)$ $If\ not\ UFP_i\ then\ terminate$ $Else:$ $UWP_i = h(UP_i \parallel UFP_i)$ $select\ T_1\ and\ a_1 \in Z^*$ $\text{NU}_i = h(UP_i \parallel UWP_i \parallel S_i)$ $SIP_i = NU_i \oplus MU_i$ $UID_i = h(UP_i \parallel a_1)$ $A_1 = h(\text{SIP}_i \parallel UID_i \parallel a_1 \parallel T_1)$ $M1 = \{A_1, UID_i, a_1, T_1\}$	
	$select\ T_2$ $check\ \|T_2 - T_1\| < \triangle T$ $A_1^* = h(\text{SIP}_i \parallel UID_i \parallel a_1 \parallel T_1)$ $if\ A_1^* \stackrel{?}{\neq} A_1$, terminate $Else:$ $select\ a_2 \in Z^*$ $SK_i = h(\text{SIP}_i \parallel a_1 \parallel a_2)$ $A_2 = h(SK_i \parallel a_2 \parallel T_2)$ $M2 = \{A_2, a_2, T_2\}$
$select\ T_3$ $check\ \|T_3 - T_2\| < \triangle T$ $SK_i^* = h(\text{SIP}_i \parallel a_1 \parallel a_2)$ $A_2^* = h(SK_i^* \parallel a_2 \parallel T_2)$ $if\ A_2^* \stackrel{?}{\neq} A_2$, terminate Else: User is authenticated	

Figure 2: Authentication phase

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

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

Security Analysis

- *Informal Security Analysis:*

The security features which achieved by the proposed protocol are:

Theorem 1: Mutual authentication is achieved between the users and HS.

Proof: In this protocol, each party (UP and HS) can trust the other and complete the session until the other party provides mathematical proof that they know the shared secret SIP_i, without sending the secret itself over the network.

- During authentication, UP_i generates and sends M1 which contains $A_1 = h(\text{SIP}_i \parallel UID_i \parallel a_1 \parallel T_1)$, when the HS receives the M1, it uses the stored value of SIP_i with the received (UID_i, a_1, T_1) to compute A_1^* , when they're matched, the HS verifies the sender's reliability.
- After the HS confirms the UP_i 's identity, it must now prove the HS's legitimacy via the M2 message. The HS calculates the session key SK_i, then derives the verification value $A_2 = h(SK_i \parallel a_2 \parallel T_2)$ and sends it to the UP_i. . The UP_i then uses the stored value SIP_i and a_1, and the received a_2 to calculate the expected session key SK_i^* and $A_2^* = h(SK_i^* \parallel a_2 \parallel T_2)$. If the value matches $A_2^* = A_2$, then the HS is authenticated, because any fake HS would never be able to calculate the correct session key SK_i due to not knowing the initial shared secret SIP_i.

Theorem2: Anonymity and untraceability are ensured

Proof: Anonymity and untraceability show that the protocol protects users' privacy (patients or doctors) against any attacker monitoring public communication channels.

During authentication, an attacker monitoring the user-server channel only observes messages M1 and M2. The user's true identity UP_i is concealed by a unique, irreversible hash $UID_i = h(UP_i \parallel a_1)$, preventing the attacker from retrieving the actual user UP_i. Even if multiple *UIDs* are intercepted from the same user across different sessions, they will vary because the random a_1 incorporated into the *UID* calculation changes in each session.

Theorem 3: The proposed protocol ensures forward and backward secrecy.

Proof: The protocol provides perfect forward secrecy because compromising current secrets does not give an attacker the mathematical ability to go back in time and decrypt stored past sessions.

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

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

Let's take the session key $SK_i = h(\text{SIP}_i \parallel a_1 \parallel a_2)$ that encrypts medical data. To decrypt an old session (for example, session number 5), an attacker needs to know the specific key for that session (SK_5). This is where the recurring random numbers (nonces) come in. Even if an attacker steals the long-term secret SIP_i today, they still need the random numbers a_1 and a_2 of that old session. Furthermore, the hash function h(·) prevents an attacker from deriving the old key SK_5 from the current key of the compromised session.

The protocol ensures strong backward secrecy because the randomly generated a_1 and a_2 values, used to create the session key, have no mathematical relationship. This randomness, combined with a hash function, makes predicting future keys impossible, even if the current key is known. Consequently, compromising a single session is isolated and cannot jeopardise medical data exchanged in subsequent sessions.

Theorem 4: Our protocol reduces eavesdropping
Proof: Eavesdropping becomes a "worthless" process for the attacker, as they obtain only randomly changing values and timestamps that do not grant them access to the system.

In eavesdropping attacks, an attacker intercepts and stores all exchanged messages (M1 and M2). Our protocol successfully neutralises this attack completely by ensuring that sensitive data and permanent secrets such as username, password, fingerprint ($UP_i, PW_i, Fing_i$), and shared secret (SIP_i) never pass through public channels explicitly. Furthermore, even if the attacker captures the authentication values and session key (A_1, A_2, SK), the mathematical properties of the hash functions prevent them from reversing the process to extract the secrets.

Theorem 5: The proposed protocol mitigates spoofing attacks
Proof: The attacker attempts to set up a fake HS to deceive users into sending their medical data to it. After the user sends message M1, the server must respond with message M2 containing the value $A_2 = h(SK_i \parallel a_2 \parallel T_2)$, where SK_i is based on SIP_i. The fake HS does not have the database containing the users' unique secrets; therefore, it cannot calculate the shared session key SK and, consequently, cannot generate the correct value A_2. The user's device will immediately detect the attack and terminate.

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

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

Theorem 6: Our protocol resists replay attacks.
Proof: In a replay attack, the attacker gains unauthorised system access by replaying or reusing a valid username and password. The protocol counters such replay attacks using two simultaneous mechanisms.:

- Utilising a timestamp in each message exchanged between Ui and HS, checking time freshness by $|T_2 - T_1| <\triangle T$ and $|T_2 - T_3| <\triangle T$ making any old message rejected because the timestamp will be outside the allowed time window ΔT.
- Using random nonces: In $M2 = \{A_2, a_2, T_2\}$ there are $A_2 = h(SK_i \parallel a_2 \parallel T_2)$ containing the unique session-specific values a_2 and T2, will prevent successful replay due to the changing nature of T1 and a_2 for each session.

Theorem 7: The proposed protocol is resistant to MITM Attacks
Proof: To prevent MITM attacks, transmitted messages require integrity and authenticity protection. During authentication, shared secret parameters SIP_i and dynamic timestamps (T_1) are combined. So, if an adversary grabs message M1, it must modify it without being detected by the HS.

However, the content parameters of $M1\ A_1\ and\ UID_i$, which are computed as $UID_i = h(UP_i \parallel a_1)$ and $A_1 = h(SIP_i \parallel UID_i \parallel a_1 \parallel T_1)$. Since the adversary is unaware of the value of SIP_i and UID_i, any modified data yields an invalid hash. Upon receiving M1, the HS will terminate the session and the verification of the condition $A_1^* \stackrel{?}{\neq} A_1$ is confirmed.

Theorem 8: Our proposed protocol effectively mitigates Denial-of-Service (DoS)) attacks and prevents resource exhaustion
Proof: Our scheme neutralises this threat through three distinct layers: first, after receiving the login request message M1, the hospital server (HS) immediately evaluates the freshness of the timestamp $check\ |T_2 - T_1| <\triangle T$. This validation requires negligible computational overhead. Second: If the incoming packet is a replayed or stale message from an attacker, the HS terminates the session instantly before invoking any resource-consuming. Moreover, the protocol relies exclusively on one-way hash functions h(·) and bitwise XOR operations. Compared to public-key cryptosystems, this allows the server to quickly reject malicious requests, preventing processing bottlenecks and server crashes. Finally, Local biometric authentication ensures no server requests are sent without confirmation.

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

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

Theorem 9: Data and Session Key Confidentiality are Guaranteed
Proof: Our designed protocol provides robust protection for sensitive session parameters and the established session key SK against any active or passive adversary monitoring the public communication channel.

During the authentication phase, the attacker can intercept the messages M1 and M2. The critical identity pseudo-parameter (SIP_i) and the secret value NU_i are never transmitted in cleartext; instead, they are masked using XOR and hash bound to secret parameters r_i or a_1. Furthermore, to compute the session key $SK_i = h(SIP_i \parallel a_1 \parallel a_2)$, an attacker needs to know SIP_i, which remains hidden and securely bound at the Healthcare Server (HS) side via the secret token a_1 in $A_1 = h(SIP_i \parallel UID_i \parallel a_1 \parallel T_1)$. Since the SHA-256 hash function is irreversible and collision-resistant, extracting SIP_i or SK from the transcript messages M1, M2 is computationally infeasible. Thus, data and session key confidentiality are strictly maintained.

Theorem 10: Message integrity is enforced
Proof: The integrity analysis ensures that any unauthorised modification, tampering, or injection of transmitted messages M1 and M2 by an adversary will be immediately detected by the receiving party.

In the proposed protocol, integrity and freshness are achieved by incorporating XOR, hash primitives and cryptographically binding all session elements. For message M1, the authentication token $A_1 = h(SIP_i \parallel UID_i \parallel a_1 \parallel T_1)$ tightly binds the user's pseudo-identity (SIP_i, UID_i), the session nonce a_1, and the current timestamp T_1. Upon receiving M1, the Healthcare Server (HS) validates the freshness via $|T_2 - T_1| < \triangle T$ and verifies integrity by recomputing A_1^*. Similarly, for message M2, the integrity token $A_2 = h(SK_i \parallel a_2 \parallel T_2)$ binds the fresh session key $SK_i$with the server's nonce a_2 and timestamp T_2. If an attacker attempts to alter any parameter (a_1, a_2 or injecting old messages), the verification equations $A_1^* = h(SIP_i \parallel UID_i \parallel a_1 \parallel T_1)$ will instantly fail, causing the protocol to terminate. Therefore, the binding of nonces and timestamps guarantees full integrity.
Table 3 summarises a comparison of related works regarding security requirements and resilience to attacks.

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

GBPA
Ghana Book Publishers Association

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

Table 3: Related works comparison

	Abbasi et al. 2024)	Abdul-Aziz Mutla et al., 2025)	(Alzahrani & Alzahrani, 2025)	Jang et al. 2026)	Lim et al. 2026)	(Almagrabi, 2026)	ours
Security features							
S1	√	√	×	√	√	√	√
S2	√	√	√	√	√	√	√
S3	√	√	√	√	√	√	√
Attacks resilience							
A1	√	×	√	√	√	√	√
A2	-	√	×	√	√	√	√
A3	-	√	×	√	√	√	√
A4	√	√	√	√	√	√	√
A5	√	×	√	×	×	×	√
A6	√	×	√	×	√	×	√

S1: mutual authentication; S2: anonymity and untraceability; S3: forward and backward secrecy; A1: replay attacks; A2: eavesdropping; A3: spoofing; A4: MITM; A5: DoS attacks; A6: impersonation.

- *Formal Proof:*

To evaluate the security robustness of the proposed protocol and guarantee that the User (Ui) and the Hospital Server (HS) achieve secure mutual authentication and session key agreement, we utilize the formal Burrows-Abadi-Needham (BAN) logic.

First: BAN Logic Notations

#(*X*): Message *X* is fresh

P|≡ *X*: *P believes the statement X.*

P|~ *X*: At some point, *P* once said *X*

P| ◁ X: *P* sees X

P| ⇒*X: P* has jurisdiction over *X*

$P \xleftrightarrow{K} Q$: P and Q share key *k*

$P \overset{K}{\rightleftharpoons} Q$: P and Q have the shared secret *k*

$\{X\}_k$: Message X is encrypted using key *k*

$\langle X_k \rangle$: Secret *k* is combined with X

Second : Idealized form of the protocol messages

Converting the protocol messages into their idealized forms:

M1) M1: $U_i \rightarrow HS$

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

GBPA
Ghana Book Publishers Association

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

Idealized form : $U_i \rightarrow HS: \{A_1, UID_i, a_1, T_1\}$

M2) $HS \rightarrow U_i$

Idealized form:) $HS \rightarrow U_i := \{A_2, a_2, T_2\}$

Third: Security Goals

The protocol must satisfy the following four core security goals between U_i and HS:

1) $U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$
2) $HS \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$
3) $U_i \mid\equiv HS \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$
4) $HS \mid\equiv U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$

Fourth: Below are the generally deployed rules of BAN logic.

R_1) Message-meaning rule (*MMR*): $\frac{P\mid\equiv P \overset{K}{\longleftrightarrow} Q, P\mid \lhd \{X\}_k}{P\mid\equiv Q\mid\equiv\sim X}$

R_2) Nonce verification rule (*NVR*): $\frac{P\mid\equiv\#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$

R_3) Jurisdiction rule (*JR*): $\frac{P\mid\equiv Q\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$

R_4) Believe rule (*BR*): $\frac{P\mid\equiv(X,Y)}{P\mid\equiv X}$

R_5) Freshness rule (*FR*): $\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$

Fifth: Assumptions of Preliminary State (APS) are formulated concerning time freshness, shared keys and nonces to prove mutuality:

APS1: $U_i \mid\equiv \#a_1$

APS2: HS $\mid\equiv \# a_2$

APS3: $U_i \mid\equiv U_i \overset{SIP}{\longleftrightarrow}$ HS

APS4: HS $\mid\equiv U_i \overset{SIP}{\longleftrightarrow} HS$

APS5: HS $\mid\equiv \# T_1$, $U_i \mid\equiv \# T_2$

ASP6: $U_i \mid\equiv$ HS $\Rightarrow a_2$

The BAN logic proof steps based on the provided codes, rules, assumptions, and ideal messages to derive the existence of secure mutual authentication between U_i and *HS* are as in follow:

1) From M1 we find that HS $\lhd$ M1 , with MMR combined with APS4, we get:

$HS\mid\equiv U_i\mid\equiv\sim M1$

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

GBPA
Ghana Book Publishers Association

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

2) Since HS knows a_1 as a part of M1 and is fresh and applying NVR with M1 freshness by the U_i and HS , this conduces that the server believes that U_i is active in the current session:

$HS \mid\equiv U_i \mid\equiv (a_1 , T_1)$

3) The SK_i is mathematically derived via $SK_i = h(SIP_i \parallel a1 \parallel a2)$, and since HS trusts M1 which contains (SIP_i and a_1), we get :

$HS \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$ (Goal 2 is formally satisfied)

4) In the same time, The HS $|\equiv U_i| \equiv \sim M1$, this fulfills Goal 4:

$HS \mid\equiv U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$

6) From M2 we get that $U_i \lhd M2$, means :

$U_i \lhd (a_2 , T_2)$

Using MMR with APS_3 we get that :

$U_i \mid\equiv HS \mid\sim (a_2 , T_2)$

7) Applying NFR and ASP_5 , The U_i ensures the message freshness:

$U_i \mid\equiv \#(a2, T2)$

8) By invoking the NVR, Ui confirms that HS is alive and currently participating in the handshake:

$Ui \mid\equiv HS \mid\equiv (a_2 , T_2)$

9) Using the JR and APS6:

$U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$ (Goal 1 is achieved)

10) From M_2 which is derived by HS, $HS \mid\equiv (a_2 , T_2)$ which forms the key, this will satisfy Goal 3:

$U_i \mid\equiv HS \mid\equiv U_i \overset{SK}{\longleftrightarrow} HS$

Since all four formal cryptographic goals of the BAN logic framework have been successfully achieved, the mathematical proof confirms that the proposed protocol establishes secure mutual authentication and guarantees a trustworthy session key agreement between the User and the Hospital Server.

A. Formal Analysis:

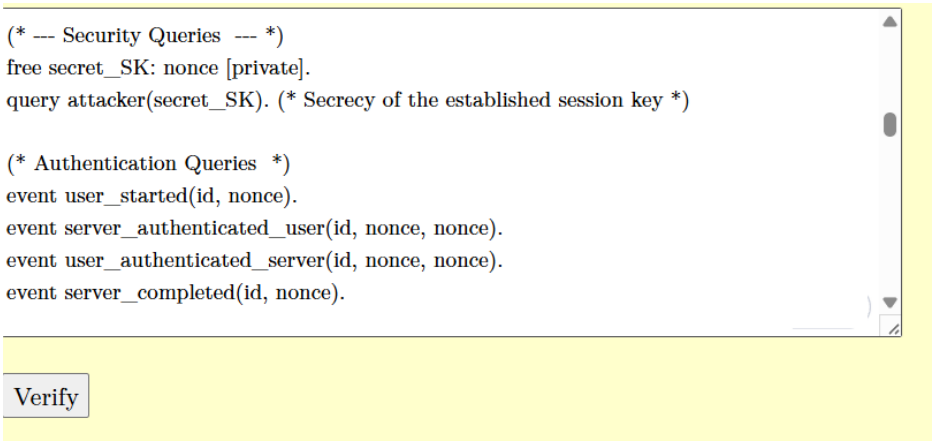
Formal Analysis with ProVerif was applied based on the "Dolev-Yao" model. This tool is used to verify cryptographic protocols formally, relying on Prologue, Horn clauses, and PI algorithms to simulate cryptographic models, public and private keys, symmetric keys, key exchange and agreement. It also provides precise notation for inference rules and expressions. It is used to show the presence of authentication, access and secrecy (Su & Xu, 2025).

Copyright ⓒ African Journal of Applied Research
Arca Academic

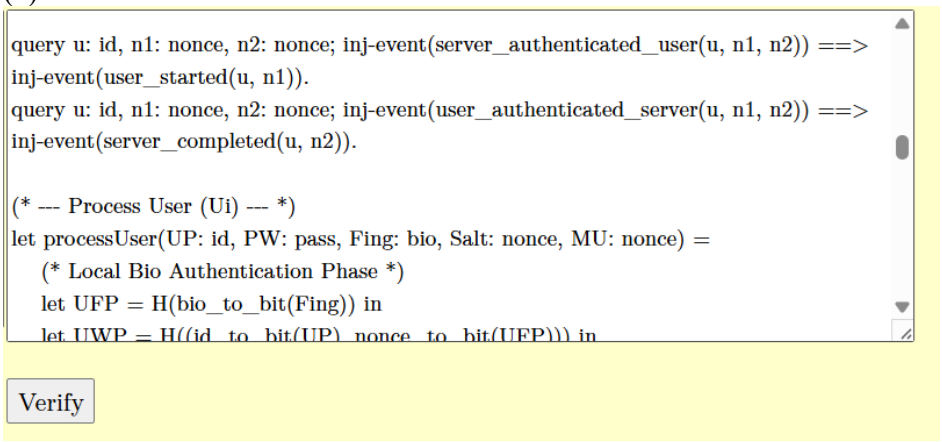
GBPA
Ghana Book Publishers Association

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

The formal analysis was applied to the authentication phase, where two entities were defined (Hospital server HS, and Users). As shown in figure(3- a,b), defining the security queries, authentication queries and a part of the user process, while In figure(4), the analysis results of the ProVerif code.



(a)



(b)

Figure 3: Parts of ProVerif code

Copyright © African Journal of Applied Research

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

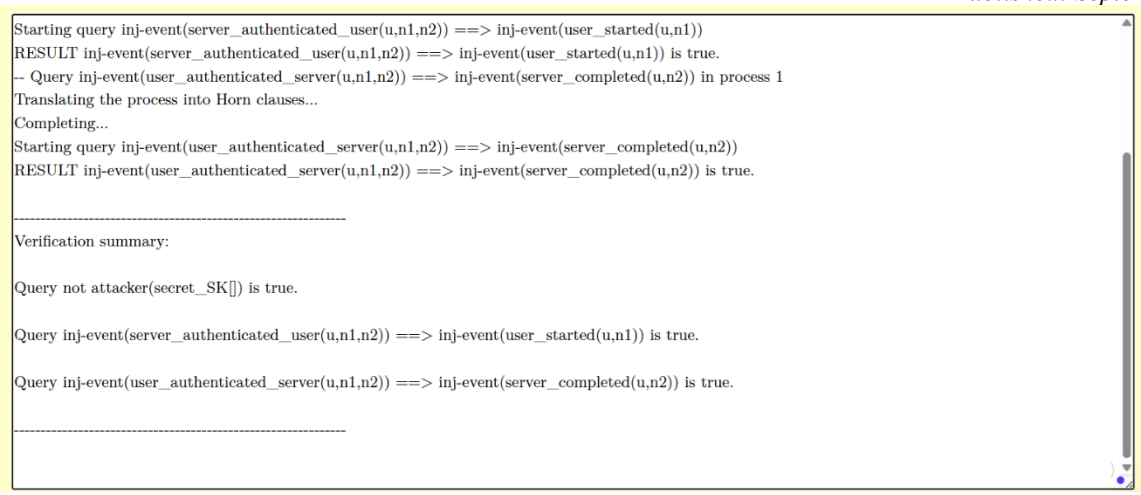


Figure 4: ProVerif results

The formal verification execution via ProVerif yields successful outputs as in Figure 4, confirming the rigorous security posture of our proposed protocol. First, the query not attacker (secret_SK[]) is true, formally proving that the negotiated session key remains completely secret against active eavesdroppers. Second, both injective correspondence authentication queries evaluate to true. This mathematically ensures robust mutual authentication in both directions, demonstrating that the protocol effectively neutralises spoofing, impersonation, MITM and replay attacks over insecure networks.

RESULTS

Security verification results. As illustrated in Figure 4, the reported ProVerif outputs return true for session-key secrecy and the two injective authentication correspondence queries. The BAN logic derivation in the preceding section addresses four stated authentication/key-agreement goals. These outcomes are bounded by the formal models and their assumptions.

Computational and communication results. The proposed scheme requires six user-side and three hospital-server hash operations, giving $9 \times 0.0025 = 0.0225$ ms under the stated benchmark. This is approximately 74.3% lower than 0.0875 ms for Abdul-Aziz Mutlaq et al. (2025). The two authentication messages total 1344 bits: 800 bits for the first message and 544 bits for the second. This equals the cost in Abdul-Aziz Mutlaq et al. (2025), exceeds Abbasi et al. (2024) at 1328 bits, and is below the other four schemes reported in Table 6.

Copyright © African Journal of Applied Research
Arca Academic

GBPA
Ghana Book Publishers Association

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

Energy results. Under the assumed 3.3 V and 15 mA energy model, a 0.0225 ms protocol execution corresponds to 1.11375 μJ. This is an analytical estimate for the stated total execution time, rather than a direct battery measurement from a wearable device. The detailed operation breakdown and comparison tables follow.

Performance Evaluation

The proposed protocol ensures secure, mutual authentication and user confidentiality in an IoHT environment. Its effectiveness was evaluated and compared against most related work in terms of communication and computational overheads and energy consumption.

A. Computational Cost

To evaluate the performance efficiency of the proposed protocol, we analyse the computational overhead incurred during the login and authentication phase. We used a Core(TM) i7-13 gen 2.40 GHz and 16 GB RAM, using Python. The execution time for each operation was calculated several times and the average was taken as a reference score. As shown in Table 4.

Table 4: Operation execution time (ms)

Symbol	Operations	Time (MS)
T_h	One-way hash	0.0025
T_f	Fuzzy Extractor	1.802
T_{ECC}	Point Multiplication of ECC	0.005
OTP	One Time Password	0.0028
$T_{c/d}$	Encryption and Decryption	0.061
T_{ascon}	Ascon algorithm	0.0024
T_{ss} / T_{ds}	Compression/ decompression	0.0023
T_{PUF}	Physical Unclonable Functions	0.0126
T_{AF}	Addition Function	0.003
T_{MF}	Multiplication Function	0.0041
T_{EF}	Exponential Function	0.0053
T_{RN}	Extraction of random number	1.12

The XOR and || operations are fast enough to be disregarded, while the Hash function takes about 0.0025 ms. In the login and authentication phase, the Ui performs 6Th calculations, while the HS calculates 3Th operations. Taking the values in Table 5, the total time of the authentication phase is (6*Th +3*Th) = (9*0.0025)= 0.0225 Ms. To evaluate our proposal versus the most related works, Table () is constructed.

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

GBPA
Ghana Book Publishers Association

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

Table 5: Computational cost comparison

Reference	Users	MS or sensors	GW: servers or gateway	Time (Ms)
Abbasi et al. 2024)	$1T_{ECC} + 6\ T_h + 1T_{c/d}$	-	$2T_{ECC} + 4\ T_h + 2T_{c/d}$	0.223
(Abdul-Aziz Mutlaq et al., 2025)	$3T_{ECC} + 8\ T_h$	$T_{ECC} + 8\ T_h$	$2\ T_{ECC} + 7\ T_h$	0.0875
(Alzahrani & Izahrani, 202	$3T_{ECC}+10T_h$	$6T_{ECC}+8T_h$	$3T_{ECC}+5T_h$	0.1175
(Jang et al., 2026)	$1T_f+2\ T_h +3T_{ascon}$	$6T_{ascon}$	$T_h +2T_{ascon}$	1.8359
(Lim et al., 2026)	$11\ T_h$	$22\ T_h + 2T_{PUF}$	$22\ T_h + 2T_{PUF}$	0.1879
(Almagrabi, 2026)	$5\ T_{AF} + 2\ T_{EF} + 7\ T_h + 2\ T_{RN}$	$3\ T_{AF} + 4\ T_h + 1\ T_{RN}$	$4\ T_{AF} + 2\ T_{EF} + 7\ T_h + 2\ T_{RN}$	5.7022
Ours	$6T_h$	-	$3\ T_h$	0.0225

Table 5 presents a comprehensive computational cost comparison between the proposed protocol and several state-of-the-art related schemes. The evaluation values show that our protocol achieves the lowest total execution time of 0.0225 ms, significantly outperforming all other schemes, mainly due to the lightweight architecture of the proposed design. While schemes like (Abdul-Aziz Mutlaq et al., 2025) and (Alzahrani & Alzahrani, 2025) rely heavily on time-consuming Elliptic Curve Cryptography (ECC) operations, schemes like (Lim et al., 2026) and (Almagrabi, 2026) introduce complex hardware-dependent primitives (such as T_{PUF}, Ascon, or T_{AF}/T_{EF}), our protocol operates strictly using ultra-fast one-way hash functions (Th).

Specifically, the User side requires only 6 Th operations, and the Hospital Server (HS) requires only 3 Th operations. Consequently, the proposed scheme reduces the total computational overhead by approximately 74.2% compared to the closest lightweight alternative (Abdul-Aziz Mutlaq et al., 2025) (0.0875 ms) and up to 99.6% compared to the heaviest scheme (Almagrabi, 2026) (5.7022 ms). This formal performance analysis proves that our protocol is highly scalable and uniquely optimised for resource-constrained IoMT devices and real-time medical applications.

B. Communication Cost :

The communication cost is calculated based on the total number of bits exchanged across the network in the various messages between connected entities during the authentication phase. The message size is calculated according to international standards (such as NIST and IETF). The exchanged messages consist of two messages: 256-bit hashes, 32-bit timestamps, and 256-bit random numbers.

Copyright ⓒ African Journal of Applied Research

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

$M1 = \{A_1, UID_i, a_1, T_1\}$ = (3×256 bits)+(1×32 bits)=768+32=800 bits, $M2 = \{A_2, a_2, T_2\}$= (2×256 bits)+(1×32 bits)=512+32=544 bits. So, the total is 1344 bits between Ui and HS to achieve mutual authentication and key establishment. Compared to traditional asymmetric or multi-message authentication protocols, an aggregate overhead of 1344 bits represents an exceptionally low communication cost. This lightweight communication cost significantly minimises network bandwidth usage and reduces transmission energy consumption, rendering our protocol highly suitable for high-throughput IoHT environments.

Table 6: Comparison of communication costs

Reference	Cost(bits)
(Abbasi et al., 2024)	1328
(Abdul-Aziz Mutlaq et al., 2025)	1344
(Alzahrani & Alzahrani, 2025)	3824
(Jang et al., 2026)	1920
(Lim et al., 2026)	3712
(Almagrabi, 2026)	4032
Ours	1344

The proposed protocol offers a highly competitive communication cost that outperforms heavy schemes (Lim et al., 2026) , (Almagrabi, 2026), and (Alzahrani & Alzahrani, 2025) by up to 66.6% in bandwidth reduction. While offering similar efficiency to lightweight schemes (Abbasi et al., 2024) and (Abdul-Aziz Mutlaq et al., 2025), the proposed protocol provides superior security, including anonymity and perfect forward secrecy, establishing an optimal balance for resource-constrained environments.

C. Energy Cost

The framework's energy efficiency was evaluated for resource-limited IoHT devices during authentication, using the energy equation described below (Sousa et al., 2024) is:

$$EN = V \times C \times EX \quad (1)$$

Where EN is energy and measured in mJ, with voltage (V) typically at 3.3 volts, current (C) at 15mA, and execution time (EX) measured in seconds. (Abood et al., 2025). The authentication phase of the U_i consumes approximately 1.11375 microjoules (μJ). As the lowest value among related works in Table 7, this demonstrates that our protocol is the most energy-efficient.

Copyright ⓒ African Journal of Applied Research

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

Table 7: Energy consumption comparison

Reference	Total Energy Consumption (μJ)
(Abbasi et al., 2024)	11.0385 μJ
Abdul-Aziz Mutlaq et al., 2025	4.3313 μJ
(Alzahrani & Alzahrani, 2025)	5.8162 μJ
(Jang et al., 2026)	90.877 μJ
(Lim et al., 2026)	9.301 μJ
(Almagrabi, 2026)	282.2589 μJ
Ours	1.11375 μJ

The evaluation reveals that our protocol incurs a very low energy overhead of 1.1138 μJ for the authentication phase, making it the most energy-efficient architecture among all related previous works in the literature. In contrast, traditional asymmetric and heavy symmetric schemes consume significantly higher energy due to their complexity and execution time. Specifically, scheme (Almagrabi, 2026) exhibits the highest energy of 282.2589 μJ, which is approximately 253 times greater than our protocol.

Furthermore, even when compared against the most competitive lightweight alternative found in scheme (Abdul-Aziz Mutlaq et al., 2025) (4.3313 μJ), our protocol reduces the energy overhead by almost 74.2%. Our protocol consumes ultra-low energy and prevents premature battery depletion in resource-constrained IoHT nodes, ensuring prolonged operational life for decentralised networks.

Discussion

The reported results suggest that the proposed protocol is computationally economical because its authentication exchange relies mainly on hashing and XOR operations rather than expensive public-key or fuzzy-extractor computations. The operation-count estimate of 0.0225 ms compares favourably with the six reported schemes, but this advantage depends on the benchmark assumptions and does not, by itself, establish equivalent speed on heterogeneous medical sensors.

The communication results should be interpreted more narrowly: the 1344-bit exchange is competitive, but not the smallest in the comparison, nor an improvement over all baselines. Specifically, Abbasi et al. (2024) report 1328 bits while Abdul-Aziz Mutlaq et al. (2025) likewise report 1344 bits. Thus, the most clearly proven benefit of the approach is its predicted computation and energy profile, not universal superiority in every performance indicator.

Copyright ⓒ African Journal of Applied Research

GBPA
Ghana Book Publishers Association

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

ProVerif results confirm secrecy and injective correspondence in the symbolic Dolev–Yao model used. They are not experimental evidence of full resilience to denial-of-service traffic, implementation defects, or biometric spoofing. Claims of perfect forward secrecy also require a separate long-term-key compromise analysis: the claimed session-key architecture employs a persistent shared value with fresh nonces, and only fresh nonces do not guarantee perfect forward secrecy if that shared value is compromised.

CONCLUSION

In this research, we proposed an ultra-lightweight cryptographic protocol for mutual authentication and session key agreement for high-throughput resource-constrained IoHT infrastructures. The protocol is carefully constructed utilising one-way hashing and bitwise XOR operations that are hardware-friendly and ultra-lightweight. Additionally, the protocol provides solid biometric privacy by confining all local biometric verification to the user's private device PSD, keeping sensitive biometric credentials within a secure local domain.

Formal security proofs using BAN logic prove the accuracy of the shared-key derivation, and automated simulations with ProVerif ensure resistance to an active Dolev-Yao adversary. The performance analysis shows the protocol's efficiency, with an ultra-low total execution time of 0.0225 ms, bandwidth utilisation of 1344 bits, and ultra-low micro-power consumption of only 1.1138 micro-joules. Finally, the proposed protocol is practical, establishing an outstanding and sustained balance between strong security resilience and hardware performance efficiency. In this paper, we present a novel approach to improve security by separating PUFs and asymmetric cryptography from user nodes. It protects the protocol against active attacks by local biometric detection, time freshness and random nonces.

In practice, the 74.2% decrease in computational overhead makes it easier to deploy on resource-limited IoHT medical devices, prolonging battery life and reducing maintenance expenses for hospitals. Socially, the protocol promotes trust in electronic healthcare systems by protecting EHRs without processing delays, thereby supporting remote patient monitoring and digitised medical services.

Future work should address several limitations. The execution benchmarks were measured on a desktop processor, the energy numbers were computed from an assumed electrical model, and no empirical fingerprint false-acceptance or false-rejection numbers were provided. The study does not disclose latency under real wireless network settings, nor does it describe scalability at high authentication volume or continuous DoS stress tests. Thus, practical validation should include

Copyright ⓒ African Journal of Applied Research
Arca Academic

GBPA
Ghana Book Publishers Association

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

embedded-device profiling, end-to-end network measurements, reproducible benchmarking with variance, biometric error analysis, and explicit compromise experiments.

Overall, the evidence supports an ultra-lightweight design with favourable estimated processing cost and successful verification of selected symbolic security properties. Broader deployment-security and scalability claims should remain provisional until validated in real IoHT settings.

REFERENCES

Abbasi, I. A., Jan, S. U., Alqahtani, A. S., Khan, A. S., & Algarni, F. (2024). A lightweight and robust authentication scheme for the healthcare system using public cloud server. *PLOS ONE*, *19*(1), e0294429. https://doi.org/10.1371/journal.pone.0294429

Abdul-Aziz Mutlaq, K., Hasson, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., Al Sibahee, M. A., Ma, J., Umran, S. M., Ali, A. H., Aldarwish, A. J. Y., & Neamah, H. A. (2025). Anonymous wireless body area networks authentication protocol based on biometrics and asymmetric key cryptography. *Array*, *27*, 100463. https://doi.org/10.1016/j.array.2025.100463

Abhishek, K., & Yogi, A. (2015). A Minutiae Count Based Method for Fake Fingerprint Detection. *Procedia Computer Science*, *58*, 447–452. https://doi.org/10.1016/j.procs.2015.08.061

Abood, E. W., Yassin, A. A., Abduljabbar, Z. A., Nyangaresi, V. O., & Ali, A. H. (2025). Provably lightweight and secure IoHT scheme with post-quantum cryptography and fog computing: A comprehensive scheme for healthcare system. *MethodsX*, *15*, 103631. https://doi.org/10.1016/j.mex.2025.103631

Abood, E. W., Yassin, A. A., Abduljabbar, Z. A., Nyangaresi, V. O., Ali, A. H., & Aldarwish, A. J. Y. (2026). Provably Ultra-Lightweight and Post-Quantum Biometric Mutual Authentication Protocol for Secure IOHT Environments. *2026 18th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1–11. https://doi.org/10.1109/ECAI69016.2026.11613778

Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2021). Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey. *IEEE Internet of Things Journal*, *8*(1), 65–84. https://doi.org/10.1109/JIOT.2020.3020076

Adel Yaseen, A., Patel, K., J. Aldarwish, A., & A. Yassin, A. (2025). An Efficient EHR Secure Exchange Among Healthcare Servers Using Light Weight Scheme. *Iraqi Journal for Electrical and Electronic Engineering*, *21*(1), 69–82. https://doi.org/10.37917/ijeee.21.1.7

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

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

Akilan, S. S., & Devprasad, K. D. (2024). Enhancing security in wireless body area networks (wbans) with ecc-based diffie-hellman key exchange algorithm (ecdh). Technology and Health Care, 32(6), 4765.

Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things*, *23*, 100844. https://doi.org/10.1016/J.IOT.2023.100844

Almagrabi, A. O. (2026). A provably secure and lightweight authentication protocol for smart home environment. *Journal of Engineering Research*. https://doi.org/10.1016/j.jer.2026.05.012

Alzahrani, A., & Alzahrani, H. A. (2025). A privacy-preserving and energy efficient authentication protocol for the cloud-based e-healthcare system. *Alexandria Engineering Journal*, *118*, 59–90. https://doi.org/10.1016/j.aej.2025.01.051

Alzaidi, Z. Sh., Yassin, A. A., Abduljabbar, Z. A., & Omollo Nyangaresi, V. (2024). Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2247–2252. https://doi.org/10.1109/CoDIT62066.2024.10708495

Chen, Y., & Chen, J. (2021). A secure three-factor-based authentication with key agreement protocol for e-Health clouds. *The Journal of Supercomputing*, *77*(4), 3359–3380. https://doi.org/10.1007/s11227-020-03395-8

Cheon, S.-P., Kang, J.-M., Park, M.-W., & Eom, J.-H. (2014). The scheme of 3-level authentication mechanism for preventing internal information leakage. *2014 Fourth International Conference on Digital Information and Communication Technology and Its Applications (DICTAP)*, 154–157. https://doi.org/10.1109/DICTAP.2014.6821674

Dang, Q. H. (2012). *Recommendation for applications using approved hash algorithms*. https://doi.org/10.6028/NIST.SP.800-107r1

Devi, R. M., Keerthika, P., Suresh, P., Sarangi, P. P., Sangeetha, M., Sagana, C., & Devendran, K. (2022). Retina biometrics for personal authentication. In *Machine Learning for Biometrics* (pp. 87–104). Elsevier. https://doi.org/10.1016/B978-0-323-85209-8.00005-5

Ding, Z., & Xie, Q. (2023). Provably secure and lightweight three-factor authentication scheme for industrial medical CPS. *Journal of Information Security and Applications*, *79*, 103656. https://doi.org/10.1016/j.jisa.2023.103656

Elhoseny, M., Ramirez-Gonzalez, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. *IEEE Access*, *6*, 20596–20608. https://doi.org/10.1109/ACCESS.2018.2817615

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

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

Hussien, Z. A., Jin, H., Abduljabbar, Z. A., Hussain, M. A., Yassin, A. A., Abbdal, S. H., Al Sibahee, M. A., & Deqing Zou. (2016). Secure and efficient e-health scheme based on the Internet of Things. *2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 1–6. https://doi.org/10.1109/ICSPCC.2016.7753621

Imamah. (2018). One Time Password (OTP) Based on Advanced Encrypted Standard (AES) and Linear Congruential Generator(LCG). *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*, 391–394. https://doi.org/10.1109/EECCIS.2018.8692931

Issad, M., Anane, N., Guenfoud, N., & Debyeche, M. (2024). HW/SW Co-Design of the Secure Hash Function SHA-256. *2024 3rd International Conference on Advanced Electrical Engineering (ICAEE)*, 1–5. https://doi.org/10.1109/ICAEE61760.2024.10783285

Jang, H., Kwon, D., & Park, Y. (2026). Ascon-Based Lightweight and Robust Authentication Scheme for IoT-Enabled Healthcare System. *IEEE Internet of Things Journal*, *13*(8), 16980–16994. https://doi.org/10.1109/JIOT.2026.3660968

Jawad, M., Yassin, A. A., AL-Asadi, H. A. A., Abduljabbar, Z. A., & Nyangaresi, V. O. (2024). *Towards Building Multi-factor Authentication Scheme for Users in the Healthcare Sector Based on Blockchain Technology* (pp. 694–713). https://doi.org/10.1007/978-3-031-70300-3_52

Lee, J., Park, J., Jung, S., & Jung, S. (2013). Advanced otp authentication protocol using pufs. In Internet 2013, The Fifth International Conference on Evolving Internet (pp. 48–51).

Ketu, S., & Mishra, P. K. (2021). Internet of Healthcare Things: A contemporary survey. *Journal of Network and Computer Applications*, *192*, 103179.

Khade, S. S., Girhepunje, V. G., Kurumbanshi, S. S., Bhoyar, D. B., Kene, J. D., Patil, A. B., ... & Prayagi, S. (2025). Advanced Miniaturised MIMO Architecture: High-Isolation Four-Element Antenna System for Next-Generation Wireless Connectivity. *African Journal of Applied Research*, *11*(6), 36-50.

Khan, A. N., Naveed, A., Mehmood, A., Arora, D., Khan, A. ur R., & Ali, J. (2025). BloomSec: Scalable and privacy-preserving searchable encryption for cloud environments. *PLOS One*, *20*(12), e0336944. https://doi.org/10.1371/journal.pone.0336944

Kim, K., Ryu, J., Lee, Y., & Won, D. (2023). An Improved Lightweight User Authentication Scheme for the Internet of Medical Things. *Sensors*, *23*(3), 1122. https://doi.org/10.3390/s23031122

Kook, S., Kim, K., Ryu, J., Lee, Y., & Won, D. (2024). Lightweight Hash-Based Authentication Protocol for Smart Grids. *Sensors*, *24*(10), 3085. https://doi.org/10.3390/s24103085

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

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

Kulikov, S. (2025). Simplest (3,2) Threshold Secret Sharing Schemes Based on EXCLUSIVE-OR Function. *Indian Journal of Cryptography and Network Security*, *5*(2), 12–16. https://doi.org/10.54105/ijcns.B1442.05021125

Lim, H., Park, Y., & Park, Y. (2026). A PUF-Based Secure and Lightweight Authentication Protocol for Medical IoT Environments. *Sensors*, *26*(10), 3223. https://doi.org/10.3390/s26103223

Martino, R., & Cilardo, A. (2020). Designing a SHA-256 processor for blockchain-based IoT applications. *Internet of Things*, *11*, 100254. https://doi.org/10.1016/j.iot.2020.100254

Qiu, X., Du, Z., & Sun, X. (2019). Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks. *IEEE Access*, *7*, 172004–172011. https://doi.org/10.1109/ACCESS.2019.2956480

Ray, P. P., Kumar, N., & Dash, D. (2021). BLWN: Blockchain-Based Lightweight Simplified Payment Verification in IoT-Assisted e-Healthcare. *IEEE Systems Journal*, *15*(1), 134–145. https://doi.org/10.1109/JSYST.2020.2968614

Sahu, A. K., Sharma, S., & Raja, R. (2022). Deep Learning-based Continuous Authentication for an IoT-enabled healthcare service. *Computers and Electrical Engineering*, *99*, 107817. https://doi.org/10.1016/j.compeleceng.2022.107817

Secure hash standard. (1995). https://doi.org/10.6028/NIST.FIPS.180-1

Shukla, S., & Patel, S. J. (2022). A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing. *Computing*, *104*(5), 1173–1202. https://doi.org/10.1007/s00607-021-01041-6

Sousa, J., Tomaz, E. B., & Araújo, A. A. (2024). Towards a Comparative Study of Authentication Mechanisms for Low-Resource Internet of Things Devices. *Anais Estendidos Do XX Simpósio Brasileiro de Sistemas de Informação (SBSI 2024)*, 369–374. https://doi.org/10.5753/sbsi_estendido.2024.238987

Su, X., & Xu, Y. (2025). An Efficient Cluster-Based Mutual Authentication and Key Update Protocol for Secure Internet of Vehicles in 5G Sensor Networks. *Sensors*, *25*(1), 212. https://doi.org/10.3390/s25010212

Villegas-Ch, W., & García-Ortiz, J. (2023). Authentication, access, and monitoring system for critical areas with the use of artificial intelligence integrated into perimeter security in a data center. *Frontiers in Big Data*, *6*. https://doi.org/10.3389/fdata.2023.1200390

Wang, L., & Han, C. (2025). Multi-factor authentication and key agreement scheme based on PUF and Chebyshev chaotic map for wireless sensor networks. *Scientific Reports*, *16*(1), 3311. https://doi.org/10.1038/s41598-025-33217-x

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

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

Yadav, A. K., Misra, M., Pandey, P. K., & Liyanage, M. (2023). An EAP-Based Mutual Authentication Protocol for WLAN-Connected IoT Devices. *IEEE Transactions on Industrial Informatics*, *19*(2), 1343–1355. https://doi.org/10.1109/TII.2022.3194956

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