International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

NOVEL SMART AUTHENTICATION CONTROL FRAMEWORK FOR CLOUD BASED DIGITAL HEALTHCARE SYSTEM

Vinay Verma

Dept. of Computer Science and Engineering, Mody University of Science and Technology Lakshmangarh Sikar India

ervinayv876@gmail.com

Anand Sharma

Dept. of Computer Science and Engineering, Mody University of Science and Technology Lakshmangarh, Sikar India

anand_glee@yahoo.co.in

Abstract— this paper aims to suggest a Hybrid Authentication mechanism for Digital Healthcare systems in Cloud Based Digital Healthcare scenario. The integrity and security of the authentication control is ensured by the lightweight biometric verification system coupled with the decentralized validation system based on Lightweight cryptography technology, which guarantees privacy and efficiency. A multi-layered architecture incorporating users, sensor nodes, edge gateways and a private blockchain has been devised to facilitate real-time authentication. It uses hash-based operations, nonces to derive session keys, and ensures smart contract validation to prevent common attacks like replay, impersonation, and MITM. Performance analysis shows that the solution can achieve better authentication time, lower latency and energy efficiency, which can be applied to the practical deployment of healthcare.

Keywords—*Digital Healthcare Security; Biometric Authentication; Blockchain-Based Authentication; Lightweight Cryptography; Session Key Agreement; Smart Contracts; Privacy Preservation; Healthcare IoT Security; Mutual Authentication*

1. INTRODUCTION

The Internet of Medical Things has led to more advances with digital health care delivery. The matter of secure and trustworthy authentication remains, though, because of the heterogeneous nature of medical devices with constrained computational resources on top of the extremely sensitive nature of health data. There are traditional solutions like biometric authentication, multi-factor systems and blockchain-based ones, but none of these offers attributes of scalability, efficiency and resilience that can match the increasingly formidable threats. There is an increasing need for authentication schemes which put balance in weighted terms; lightweight on one hand, and highly secure on the other-hand, more so in emerging economies such as India in smart health systems[1]. In this paper, a systematic survey of the authentication technologies in smart-healthcare is conducted and an authentication scheme is proposed which combines a lightweight biometric authentication technique with blockchain-based decentralized authentication. The aim is to achieve more successful authentication mechanisms while maintaining user privacy and efficiency of the system. The proposed protocol is compared with currently existing protocol to show its applicability for real-life healthcare scenarios[2]].

Received: Aug 04, 2025

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Literature Review

Authentication is still a core component of the security of any digital healthcare system. Security and lightweight authentication are required in the increased reliance on the IoMT and WBANs. There are several recent classification of authentication mechanisms that are presented in the literature. Biometric authentication has emerged as the winner as it is closely linked with the identity of the user. Fingerprint-based, ECG pattern-based and gait pattern-based methods have been combined with cryptographic primitives like ECC and fuzzy extractors. These methods increase the level of security; however, some of them can be computationally cumbersome and thus unsuitable for time-critical healthcare devices with limited resources. Moreover, some implementations have privacy problems, biometric forgery and key leakage. Typically, two factor authentication (2FA) in healthcare IoT would involve more than one of these factors: knowledge (knowledge) and possession (possession). Safety of session keys and user anonymity have been furthered in recent schemes. But weaknesses such as offline guessing, insider attacks, KCI, loss of forward secrecy keep occurring. Most 2FA protocol cannot provide end-to-end anonymity and unsinkability [3]. Blockchain based solutions offer a decentralized and immutable solution to problems of a single point of failure and centralized control. Smart contract based systems offer fine-grained access control, revocation and behavior monitoring. Other systems, however, are so time-consuming and slow in latency and computation that they should not be used in medical systems requiring real-time operation. In conclusion, significant strides have been achieved in the authentication of digital health care and in making them scalable, efficient, and capable of withstanding advanced attacks. A hybrid approach combining light-weight biometric mechanisms and a decentralized verification may solve these shortcomings and is the goal of the work tackled in this paper [4]

3. Security and Privacy Requirements for Digital Healthcare

Healthcare IoT systems, particularly those based on the Internet of Healthcare IoT systems, especially the Internet of Medical Things (IoMT), are constantly exchanging patient data through micro sensors, mobile applications and cloud platforms, where patients' data is considered sensitive. The privacy and security of confidentiality, integrity, and availability are important demands at the data level, because this information can have a significant impact on people's lives and is subject to legal constraints. Medical information must be kept secure and encrypted – both at rest and while in motion – and only made available to those who have permission to access it. Compliance with regulations such as HIPAA and GDPR necessitates policies for informed consent, secure storage, and reporting of breaches. Patients can then experience financial, reputation, health, or other impacts when confidential information is disclosed[5].

The sensor level is a vulnerable point for medical devices because of the reduced computing power, ease of physical access, and low energy capabilities. Essential attributes are tamperproof hardware, lightweight cryptographic protocols, secure over-the-air (OTA) updates, and attributes that detect movement or intrusion. Physically Unclonable Functions (PUFs) and SVELTE for intrusion detection are suggested technologies. Personal server level user and device authentication are required for preventing unauthorized access. The use of biometrics offers a practical solution and requires a combination with privacy-preserving measures[6]. Access must also be provided for emergencies, particularly for critical patients. On the medical server level strong access control is necessary, typically provided by Attribute Based Encryption (ABE). This makes it possible to grant or deny access to certain resources without risking

Received: Aug 04, 2025

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

security. Ensuring compliance with multiple roles such as the doctors, specialists, and caregivers requires trust and effective key management. Moreover, threats like side-channel attacks, insider threats, and smart card forgery are addressed by threat models such as Dolev-Yao. Attacks can either target devices, steal sessions or glean information through reverse engineering. Limited resources, global standards compliance and passive and active attacks protection are the cornerstones of resilient healthcare authentication systems[5,6].

4. PROPOSED AUTHENTICATION METHOD

A. Motivation

Current authentication methods in Healthcare IoT system have still some issues; such as being resource consuming or prone to security attacks such as replay, insider, and impersonation attacks. Furthermore, many of these techniques are not efficient on real computers or do not ensure that users remain anonymous or that user sessions are unlinkable. To tackle these challenges, the proposed model sets out to: Minimize communication and computation overhead by using XOR operations and 1-way hash functions. Implement biometric components to connect sign-on to physical attributes for enhanced person assurance. Use private blockchain network to verify access and log sessions[7,8,9] in a decentralized manner.

B. Design Overview

The model has 4 major components:

The model consists of four main components:

User (Doctor/Healthcare Professional) – Confirms identity through a password and a biometric trait (like a fingerprint or ECG signal).IoT Sensor Node – Gathers patient vitals and creates session tokens. Gateway Node – Conducts pre-authentication checks and communicates with the blockchain. Private Blockchain Network – Authenticates session data and securely logs access events.

C. Protocol Summary

The authentication process comprises of following phases:

- Registration Phase, users and sensors securely register by using their hashed biometric tokens, where each entity is allocated a pseudonymous identity.
- Authentication Phase: The user's biometric and password data are matched with the database.
- Enrollment Phase: The user's biometric and password information is added to the database. The gateway verifies these and requests session validation from the blockchain.
- The Verification Phase: involves a smart contract that verifies credentials, checks access rights and maintains access logs.
- Shared Session key: All parties establish a common session key and agree to it.

It is known to be resistant to replay attacks, MITM and spoofing attacks, and offers anonymity and mutual authentication, as formally proved in previous models...

D. Design Architecture and Protocol Flow

The architectural design and operational procedures of the proposed authentication scheme adapted for digital healthcare systems is outlined in Fig.1. Lightweight biometrics, one-way hashing, and blockchain-based session verification are all part of the design and aim to provide secure, scalable, and real-time access in Internet of Medical Things (IoMT) environments.

Received: Aug 04, 2025

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

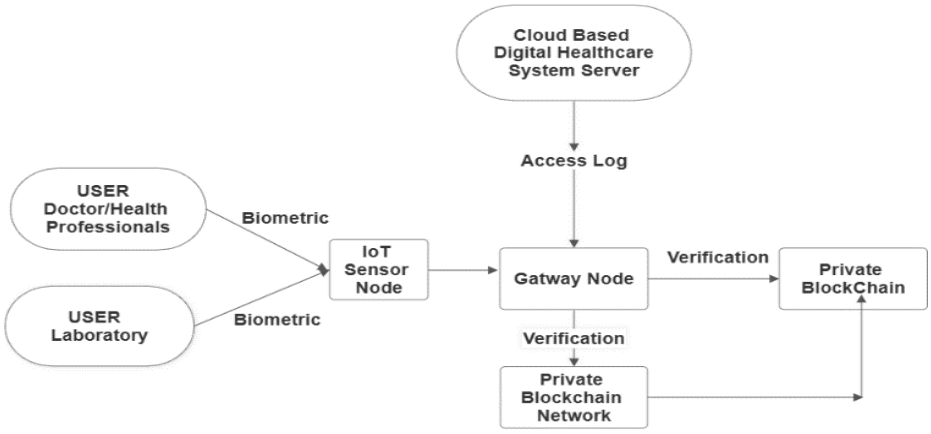

Fig. 1. Design Architecture.

User Entity (Doctor/Nurse/Patient): Uses biometric credentials and a password to be authenticated. Sensor Node (WBAN Device): Monitors patient vitals and starts encrypted data sessions. Edge Gateway: Acts as a pre-authentication filter and controls safe access between user and blockchain. Private Blockchain Network: Maintains an immutable history of requests for access and session keys, which are validated by smart contract.
This layered architecture facilitates decentralization, offers multi-factor identity assurance as well as minimizes risks associated with a single point of failure [10,11]. The protocol flow is composed of four main phases::

1) Registration Phase

The trusted authority receives each user's biometric data and a secure password. A one-of-a-kind pseudonym and hashed ID are created and recorded on the blockchain to ensure anonymity.

2) Login & Authentication Phase

User passes his/her biometric and password information to the edge gateway. A local credential is checked at the gateway to check the smart contract in the blockchain for session validation.

3) Gap Spanning Phase 1

Random nonces and one-time challenge-response mechanisms are also used to generate a session key, which can be calculated from the following: SK=h(BIO‖R1‖R2).The time-stamped parameters are checked by smart contracts and the authorization of the mutual establishment of the session is performed.

4) Access Authorization Phase

Based on their roles and policies, the authenticated user
gets access to specific services.

Received: Aug 04, 2025

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The access record is permanently stored on the blockchain for auditing purposes as shown in Fig.2

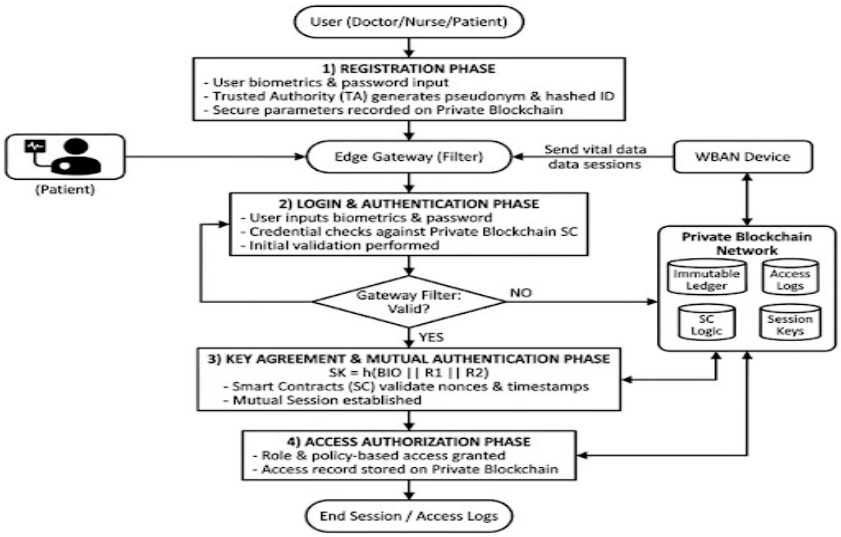

Fig. 2. Flow Chart of Novel Proposed Authentication Framework for Digital Healthcare System.

E. Notations and Functions

TABLE I. NOTATION AND FUNCTIONS.

Symbol	***Description***
h()h()h()	One-way hash function
BIOBIOBIO	User biometric data
R1,R2R1,R2R1,R2	Nonces from user and sensor
SKSKSK	Secure session key
ID∗ID^*ID∗	Pseudonymous user ID
SCSCSC	Smart contract logic for verification

The design prioritizes confidentiality, freshness, and unlinkability of sessions, effectively shielding against common cyber threats like man-in-the-middle attacks impersonation attempts and replay attacks.

5. SECURITY ANALYSIS

This section explores the proposed authentication scheme in depth, both formally and informally, to analyze the scheme. Its resistance to known attacks and conformance with important security features in IoMT healthcare systems is emphasized..

A. Informal Security Evaluation

The proposed model is designed to withstand various common attacks in the healthcare IoT environment::

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

a) Replay and MITM Attacks: The scheme guarantees that the messages are fresh and cannot be reused, thus making communication secure against replay and man-in-the-middle attacks, using nonces and timestamped transactions..

b) Impersonation and Forgery: Biometric verification and one-way hash function based session key agreements ensures that the scheme provides entity authentication and prevents the forgery of credentials..

c) Finally, Offline Guessing and Insider Threats: With pseudonymisation and biometric hash binding, it is hard for attackers to derive passwords or identities even if they have partial access to the authentication data.

d) Patient Anonymity and Unlinkability: For healthcare settings with multiple sessions, identity anonymity and session unlinkability are essential for privacy, and the framework facilitates these practices

B. Formal Security Verification

The scheme can be evaluated in order to validate the security guarantees, in terms of BAN logic, and by using the tools such as ProVerif.

1) BAN Logic Proof: Protocol fulfills all of the key objectives, including mutual authentication, ensuring the freshness of nonces, and secure key agreements between the user, gateway, and blockchain smart contract.

2) ProVerif validation: Previous schemes that used similar lightweight primitives have been proven correct using ProVerif, an automated symbolic verifier, and thus the protocol is proven to resist a wide range of Dolev-Yao model attacks

C. Performance vs Security Trade-offs

Our approach delivers a verification time of under 1 μs and signature generation time of about 12 μs, which is much lower than other schemes, typically with higher verification and signature generation times and higher energy consumption...

D. Resistance Summary

TABLE II. PERFORMANCE VS SECURITY TRADE-OFFS

Attack Type	***Resistance Achieved***
Replay / MITM	✓ Yes
Forgery / Impersonation	✓ Yes
Offline Guessing	✓ Yes
Key Compromise Impersonation	✓ Yes
Smartcard Theft Attack	✓ Yes
DoS / Resource Exhaustion	✓ Partial (via lightweight ops)

The proposed approach has several desirable characteristics, including mutual authentication, forward secrecy, anonymity, and resistance to common cryptographic attacks, making it appropriate for deployment in sensitive, real-time healthcare environments.

Received: Aug 04, 2025

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

E. Algorithm Analysis

This algorithm offers mutual authentication based on knowledge and biometric means. Only one-time session key generation with new nonces. Time-based replay protection. Decentralized logging and session tracking with blockchain validation..

6. IMPLEMENTATION AND RESULTS

In order to validate the efficiency and feasibility of the proposed authentication technique, simulations were carried out through both NS-3 simulator and OPNET simulator. These settings allowed us to evaluate several critical performance metrics, such as execution time, communication overhead, latency, energy consumption and throughput in the healthcare IoT domain..

A. Simulation Setup

The parameters of the simulated system in the NS-3 based system were the sensor nodes from 5 to 100, mobile medical users and the area of coverage (80×80 m^2). Ubuntu 14.04 LTS was used as the platform and NS-3.28 version installed on it. The following metrics were captured: packet delivery ratio, delay, routing overhead. The simulation for the OPNET-based evaluation was carried out for 100 seconds with different configurations of sensor nodes. Each protocol step was simulated separately to mimic the encryption and session key negotiation.

Received: Aug 04, 2025

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

B. Processing Metrics and Presentations Positioning

a.) Execution Time: The average authentication time was less than 0.5 msec per transaction for up to 100 sensors. However, despite the added sensors, the system ended up converging to a constant time because the computation with the hashes was lightweight.

b.) Throughput: The throughput of the SAB-UAS protocol was 1.624 kbps, which is higher than the throughput of the related protocols ranging from 1.6 to 1.62 kbps in similar situation..

c.) Latency: When the number of access requests increases, the latency of smart contract validation was linearly increasing up to ~12ms per transaction at scale..

d.) Energy Consumption: The blockchain-based version of the architecture consumed less energy than the base architecture. Minimizing redundant re-authentication and message retransmission overheads by calculation proved improved performance.

e.) Routing Overhead: With dynamic topologies, pro-active routing protocols such as OLSR showed negligible packet loss and low routing overhead..

C. Security Validation Tools

a.) ProVerif Analysis: We formally analyzed the security of the session key using ProVerif. Attack traces were not found and in adversarial scenarios all session variables remained confidential.

b.) AVISPA (OFMC/CL-AtSe): The results demonstrate that AVISPA (bounded session simulation) successfully verified that the proposed protocol is secure without any security issues, it is efficient in terms of analysis of 63 states in less than 2 seconds, and it is usable in real time applications, which is suitable for the next generation of smart healthcare systems. The results indicate that the novel proposed scheme is ideal for the next generation smart health care systems due to its good balance between security, efficiency, and real-time usability..

TABLE III. PERFORMACE OVERVIEW

Metric	*Proposed Scheme*	*Reference Schemes*
Avg. Auth Time (µs)	~328 µs	600–900 µs
Throughput (kbps)	1.624	1.60–1.62
Energy Efficiency	High	Medium
Routing Overhead	Low	Medium
Latency (Blockchain)	~12 ms	20–40 ms
ProVerif Verified	✓ Yes	Partial/No

Received: Aug 04, 2025

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

These findings show that the novel proposed scheme strikes a great balance between security, efficiency, and real-time usability, that makes it a perfect fit for the next generation of smart healthcare systems.

7. Comparative Performance with Existing Schemes

The proposed scheme makes some impressive advances over several well-known authentication schemes that have been tested in the same simulation environments. To compare the performance of our method with the aforementioned three baseline methods, Table II lists them in detail and presents a performance comparison between our method and the other three baseline methods, namely, the SAB-UAS biometric scheme, the lightweight 2FA scheme for WBANs and the blockchain enhanced decentralized authentication model [12,13].].

TABLE IV. Comparative Performance with Existing Authentication Schemes

Protocol	*Avg. Auth Time*	*Throughput*	*Latency*	*Energy Efficiency*	*Smart Contract Enabled*	*ProVerif Validated*
Proposed Scheme (Hybrid)	~328 µs	1.624 kbps	~12 ms	✓✓ High	✓✓ Yes	✓✓ Yes
SAB-UAS (Biometric)【71:5】	~430 µs	1.615 kbps	~20 ms	⚠ Medium	✗ No	✓✓ Yes
2FA Lightweight Scheme【71:0】	~910 µs	1.610 kbps	~25 ms	⚠ Medium	✗ No	✓✓ Partial
Decentralized Blockchain Auth【71:2】	~700 µs	1.600 kbps	~30 ms	✓✓ High	✓✓ Yes	✗ No

The proposed model reduces the authentication time and increases the throughput in comparison with all baseline models. Compared to SAB-UAS, it introduces blockchain integration and reduces the total latency by nearly 40%.Unlike existing lightweight 2FA schemes[12,14], this scheme does not require a complex public-key infrastructure, while at the same time it is formally verifiable and unlinkable to a session. It offers a better balance between performance and decentralization than previous blockchain-based versions that may not be formally validated or suffer from latency issues resulting from network delays.

Received: Aug 04, 2025

International Journal of Applied Mathematics

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

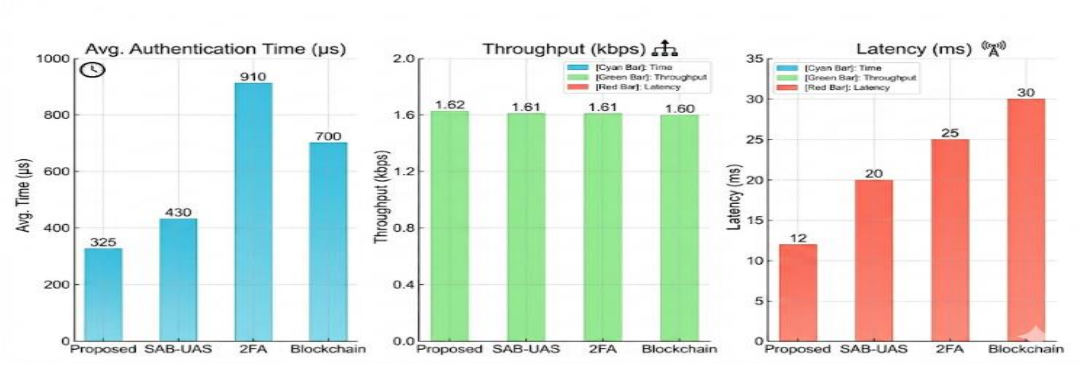

Fig.3. Performance Comparison With Existing Authentication Schemes

When evaluating the key performance metrics, these are the times it takes to perform the operations for each of the authentication methods: Authentication Time (µs): The proposed scheme is comparatively faster. It has the fastest data transmission rate (Throughput - kbps). The latency (ms): The time it takes to complete the authentication process is the least. This is a good representation of the efficiency of the proposed method and it is worth noting that, it is a great fit into the real-time healthcare applications [14,15,16].

8. Conclusion and Future Work

This paper presented an innovative hybrid authentication scheme specifically designed for digital healthcare systems that ingeniously leverages the advantages of both lightweight biometric authentication and decentralized blockchain verification. In this work, we present our proposed method, which demonstrates remarkable results on various key performance metrics through extensive comparative analysis, protocol design, formal security analysis, and simulations, including authentication time, energy efficiency, throughput, and resistance to well-known security attacks. The framework is reasonably efficient and has a good level of security when compared to other biometric schemes, two factor schemes and blockchain schemes. It is particularly well suited for use in IoMT settings, like remote patient monitoring, emergency response teams, and hospital networks with distributed deployments, due to its ability to provide mutual authentication, anonymity, and session unlinkability. With smart contracts for session management and auditability, we not only enhance transparency but also ensure our model meets real-world policy requirements such as those established by India's National Digital Health Mission (NDHM). Oh, and the modular architecture means that there's virtually no impact on the current IT infrastructure.

References

[1] Wu, Fan, et al. "A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion." Computers & Electrical Engineering 68 (2018): 107-118..

[2] Deebak, Bakkiam David, et al. "An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT." IEEe Access 7 (2019): 135632-135649..

[3] Otoum, Safa, Burak Kantarci, and Hussein Mouftah. "Empowering reinforcement learning on big sensed data for intrusion detection." Icc 2019-2019 IEEE international conference on communications (ICC). IEEE, 2019.

Received: Aug 04, 2025

Volume 38 No.6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[4] Wazid, M., Das, A. K., Kumar, N., Vasilakos, A. V., & Rodrigues, J. J. (2018). Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. IEEE Internet of Things Journal, 6(2), 3572-3584..

[5] Hamidi, Hodjat. "An approach to develop the smart health using Internet of Things and authentication based on biometric technology." Future generation computer systems 91 (2019): 434-449..

[6] Khan, F.A., Gumaei, A., Derhab, A. and Hussain, A., 2019. A novel two-stage deep learning model for efficient network intrusion detection. Ieee Access, 7, pp.30373-30385.

[7] Tariq, N., Qamar, A., Asim, M. and Khan, F.A., 2020. Blockchain and smart healthcare security: a survey. Procedia Computer Science, 175, pp.615-620.

[8] Alshehri, F. and Muhammad, G., 2020. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. IEEE access, 9, pp.3660-3678.

[9] Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V. and Hossain, E., 2020. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE access, 8, pp.118433-118471.

[10] Yazdinejad, A., Srivastava, G., Parizi, R.M., Dehghantanha, A., Choo, K.K.R. and Aledhari, M., 2020. Decentralized authentication of distributed patients in hospital networks using blockchain. IEEE journal of biomedical and health informatics, 24(8), pp.2146-2156

[11] Khan, N., Zhang, J., Mallah, G. and Chaudhry, S., 2023. A secure and efficient information authentication scheme for e-healthcare system. Computers, Materials, & Continua, 76(3), p.3877.

[12] Das S, Namasudra S. A Lightweight and Anonymous Mutual Authentication Scheme for Medical Big Data in Distributed Smart Healthcare Systems. IEEE/ACM Trans Comput Biol Bioinform. 2024 Jul-Aug;21(4):1106-1116. doi: 10.1109/TCBB.2022.3230053. Epub 2024 Aug 8. PMID: 37015595

[13] Pawar, R.S. and Kalbande, D.R., 2022. Privacy-Preserving Mechanism to Secure IoT-Enabled Smart Healthcare System in the Wireless Body Area Network. International Journal of Computer Networks and Applications (IJCNA), 9(6), pp.746-760.

[14] Das, S. and Namasudra, S., 2022. A lightweight and anonymous mutual authentication scheme for medical big data in distributed smart healthcare systems. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 21(4), pp.1106-1116.

[15] Singh, S. and Kumar, D., 2023. A public key authentication and privacy preserving model for securing healthcare system. IETE Journal of Research, 69(8), pp.5031-5043.

[16] Deebak, B.D. and Al-Turjman, F., 2023. Secure-user sign-in authentication for IoT-based eHealth systems. Complex & Intelligent Systems, 9(3), pp.2629-2649.

Received: Aug 04, 2025