International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

*Full Length Article*

# An Medical Data A User Authentication Of A Cloud Data

**Mohammed Omer Shaik[1], Saif Ahmed[2], Mohammed Abdul Kaleem Ansari[3], Mr. Diwakar Tiwary[4]**
[1,2,3]B.E.Students; Department of CSE (Artificial Intelligence And Data Science) ISL Engineering College Hyderabad India
[4] Assistant Professor; Department of CSE (Artificial Intelligence And Data Science) ISL Engineering College Hyderabad India
Mail Id; omershaikmohammed@gmail.com , Saif1024p@gmail.com , 160522747059@islec.edu.in
***Accepted 25-04-2026***


***ABSTRACT:***
*With the rapid adoption of cloud computing in healthcare, securing medical data stored and accessed through cloud platforms has become a critical priority. Unauthorized access to sensitive health records can lead to severe privacy violations and misuse of patient information. Therefore, robust user authentication mechanisms are essential to ensure that only legitimate users can access or modify medical data in cloud environments. This paper presents a secure and efficient user authentication scheme tailored for cloud-based medical systems, focusing on protecting data integrity and ensuring user privacy. The proposed scheme employs a multifactor authentication model that integrates otp verification, cryptographic credentials, and device-based factors to authenticate users accessing electronic health records (EHRs). To counter emerging threats, especially from quantum-capable adversaries, the protocol incorporates post-quantum cryptographic techniques, ensuring long-term security resilience. The protocol is formally verified using the ProVerif tool and evaluated against standard security criteria, demonstrating resistance to attacks such as replay, man-in-the-middle, insider threats, and stolen-verifier attacks. Furthermore, performance analysis confirms the protocol's low computational and communication overhead, making it suitable for real-time medical applications. The results highlight the protocol's ability to maintain a secure and scalable framework for confidential medical data access in cloud environments, balancing security, usability, and efficiency*

***Keywords—*** *Cloud Computing, Healthcare Security, User Authentication, Electronic Health Records (EHR), Multi-Factor Authentication, Post-Quantum Cryptography, Cloud-Based Medical Systems, ProVerif, Data Privacy, Secure Access Control.*

## Introduction

The rapid advancement of information technology and the increasing adoption of cloud computing have transformed the healthcare industry by enabling efficient storage, processing, and management of medical information. Healthcare institutions such as hospitals, clinics, diagnostic centers, pharmacies, and research organizations increasingly rely on digital platforms to maintain Electronic Health Records (EHRs), patient histories, diagnostic reports, prescriptions, billing information, and treatment plans. Cloud computing has emerged as a powerful technological solution because it offers on-demand access to computing resources, scalable data storage, cost efficiency, and improved accessibility. Through cloud platforms, healthcare providers can access patient information remotely, collaborate across different geographical locations, and deliver healthcare services more efficiently.

In modern healthcare environments, the Medical Internet of Things (MIoT) has become a major contributor to digital healthcare transformation. MIoT consists of interconnected medical devices, wearable sensors, smart monitoring equipment, and communication technologies that continuously collect physiological information from patients. These devices monitor parameters such as heart rate, blood pressure, oxygen levels, body temperature, glucose levels, and other vital medical conditions. The collected data is transmitted to healthcare servers and cloud platforms for real-time monitoring, analysis, diagnosis, and medical decision-making. Cloud-assisted healthcare systems allow doctors, nurses, caregivers, and authorized healthcare professionals to access patient information anytime and anywhere, improving the quality and speed of medical services.

Despite these advantages, cloud-enabled healthcare systems face serious security and privacy challenges. Medical information is highly sensitive and confidential, and unauthorized disclosure may result in privacy violations, identity theft, insurance fraud, medical manipulation, financial loss, and reputational damage. Since communication between medical devices, users, and cloud servers occurs through public networks, healthcare systems are vulnerable to various cybersecurity threats. Attackers may exploit network vulnerabilities to perform replay attacks, impersonation attacks, insider attacks, man-in-the-middle attacks, stolen-credential attacks, and unauthorized data access. These attacks can compromise the confidentiality, integrity, and availability of medical information.

Traditional authentication and cryptographic mechanisms such as RSA and Elliptic Curve Cryptography (ECC) have long been used to secure



https://doi.org/10.63665/IJMEC.1104s.54
ISSN: 2456-4265
IJMEC 2026

communication and authenticate users in digital systems. However, recent developments in quantum computing have created significant concerns regarding the long-term security of these conventional cryptographic approaches. Quantum algorithms, particularly Shor's Algorithm, demonstrate the potential to solve factorization and discrete logarithm problems efficiently, threatening the security foundations of traditional public-key cryptography. Consequently, there is a growing demand for next-generation authentication systems capable of resisting both classical and quantum-based attacks.

To address these challenges, the proposed work introduces a secure cloud-based medical authentication framework that combines multifactor authentication, post-quantum cryptographic techniques, and secure access control mechanisms. The proposed framework aims to protect Electronic Health Records, maintain user privacy, ensure secure communication between healthcare entities, and provide long-term security resilience against emerging quantum threats. By integrating OTP verification, device-based authentication, cryptographic credentials, and post-quantum security measures, the system establishes a secure, reliable, and scalable authentication environment for cloud-enabled healthcare applications.

**Motivation and Problem Statement**

The motivation for this project originates from the rapid digital transformation taking place in the healthcare sector and the increasing dependence on cloud computing technologies for storing, processing, and sharing medical information. Modern healthcare systems generate enormous amounts of patient-related data, including medical histories, laboratory reports, diagnostic images, prescriptions, insurance details, treatment plans, and billing records. Managing such a large volume of information through traditional paper-based systems or isolated software platforms has become increasingly inefficient and difficult. Cloud computing offers an effective solution by enabling centralized storage, scalable infrastructure, remote accessibility, and efficient healthcare service management. However, the migration of sensitive healthcare data to cloud environments introduces significant concerns related to security, privacy, trust, and access control.

One of the major motivations behind this work is the increasing frequency of cybersecurity attacks targeting healthcare organizations worldwide. Healthcare data is extremely valuable because it contains personal identification information, medical histories, financial details, and insurance records. Unauthorized access to such information can result in privacy violations, identity theft, insurance fraud, medical data manipulation, and financial losses. In many cases, compromised medical information can also affect patient treatment quality and clinical decision-making. Therefore, securing healthcare information is not only a technological requirement but also a critical necessity for maintaining patient safety, trust, and regulatory compliance.

Many existing healthcare systems still depend on fragmented software applications, manual workflows, and isolated databases that lack centralized coordination. These limitations create several operational problems including data redundancy, inconsistent records, delayed information retrieval, and poor communication among healthcare stakeholders. Patients often experience difficulties in accessing medical reports, obtaining prescriptions, scheduling consultations, and tracking treatment information. Similarly, healthcare providers may face challenges in managing doctor approvals, billing systems, medicine inventories, patient monitoring, and secure information exchange. The absence of a unified and secure healthcare management framework negatively affects service efficiency and decision-making processes.

Another important concern is the growing complexity of cyber threats in cloud-assisted healthcare environments. Traditional authentication systems based solely on passwords or single-factor verification are increasingly vulnerable to phishing attacks, replay attacks, credential theft, insider attacks, and impersonation attempts. Attackers can exploit weak authentication mechanisms to gain unauthorized access to Electronic Health Records and confidential medical resources. Furthermore, future developments in quantum computing present a serious threat to conventional cryptographic systems such as RSA and Elliptic Curve Cryptography, which are widely used for authentication and secure communication.

The problem addressed by this project is therefore the lack of a secure, scalable, and future-ready authentication framework capable of protecting cloud-based healthcare systems against both current and emerging cybersecurity threats. Existing solutions often fail to provide strong multifactor authentication, quantum-resistant security, efficient performance, and comprehensive access control within a unified environment. To overcome these limitations, the proposed system introduces a secure cloud-assisted healthcare framework that integrates multifactor authentication, post-quantum cryptographic protection, role-based access management, and formal security verification. The objective is to establish a robust authentication environment that ensures secure user access, data confidentiality, privacy preservation, and reliable healthcare service delivery.

**Literature Survey on Post-Quantum Healthcare Security**

The integration of cloud computing, Medical Internet of Things (MIoT), and digital healthcare technologies has motivated extensive research in healthcare cybersecurity and authentication mechanisms. Researchers have proposed several authentication frameworks to secure communication between patients, doctors, healthcare servers, wearable medical devices, and cloud infrastructures. Traditional healthcare authentication methods primarily relied on password-based systems for



https://doi.org/10.63665/IJMEC.1104s.54
ISSN: 2456-4265
IJMEC 2026

user verification. Although these approaches were simple and easy to implement, they exhibited several security weaknesses, including vulnerability to password guessing attacks, replay attacks, phishing attacks, and credential theft. Due to the limitations of single-factor authentication, researchers began exploring stronger and more resilient security approaches.

Multi-factor authentication techniques emerged as an effective solution for improving healthcare security. Several research studies introduced authentication frameworks that combine multiple verification factors such as passwords, smart cards, biometric information, One-Time Passwords (OTP), and device credentials. These systems provide improved resistance against unauthorized access, impersonation attacks, insider threats, and stolen credential misuse. By requiring multiple authentication factors, such frameworks strengthen identity verification and reduce dependency on a single security parameter.

In cloud-assisted healthcare and Internet of Medical Things (IoMT) environments, authentication and key agreement protocols have gained substantial research attention. Authentication Key Exchange (AKE) protocols are widely used to establish secure communication channels between healthcare entities and cloud servers. Many researchers have proposed lightweight authentication protocols specifically designed for resource-constrained healthcare devices such as wearable sensors, implantable devices, and remote monitoring systems. These protocols generally aim to achieve mutual authentication, secure session key establishment, data integrity, and confidentiality while minimizing communication overhead and computational complexity.

Cryptographic techniques play a central role in healthcare authentication systems. Researchers have applied methods such as public-key cryptography, hash-based authentication, digital signatures, elliptic curve cryptography, and identity-based cryptographic schemes to protect healthcare information. Elliptic Curve Cryptography gained significant popularity due to its strong security characteristics and relatively lower computational requirements compared with traditional cryptographic methods. However, recent advances in quantum computing have raised concerns regarding the long-term viability of conventional cryptographic algorithms. Quantum algorithms such as Shor's Algorithm demonstrate the ability to compromise RSA and ECC by efficiently solving factorization and discrete logarithm problems.

To address these emerging threats, researchers have increasingly focused on post-quantum cryptography. Post-quantum cryptographic techniques are specifically designed to resist attacks from quantum-capable adversaries while maintaining practical security performance. Several categories of post-quantum algorithms have been explored in healthcare security research, including lattice-based cryptography, code-based cryptography, multivariate cryptography, and hash-based cryptographic constructions. Among these approaches, lattice-based cryptography has gained particular attention because of its strong theoretical foundations, computational efficiency, and suitability for secure authentication systems.

Recent studies have also investigated the integration of biometrics with post-quantum cryptographic methods to improve authentication reliability and user convenience. Biometric authentication techniques such as fingerprint recognition, iris scanning, facial recognition, and voice verification provide unique user identification capabilities. When combined with post-quantum cryptographic protection, biometric authentication frameworks offer enhanced resistance against credential compromise, replay attacks, and identity theft. Fuzzy commitment schemes and biometric template protection mechanisms have been proposed to securely bind biometric features with cryptographic keys while tolerating natural biometric variations during authentication.

Formal verification methods have also become an important area of healthcare security research. Tools such as ProVerif, AVISPA, and BAN logic are frequently employed to validate authentication protocols and analyze their resistance against various cyberattacks. Formal verification allows researchers to mathematically verify critical security properties including secrecy, authentication correctness, session key confidentiality, forward secrecy, and attack resilience. By identifying vulnerabilities during the design stage, formal analysis significantly improves protocol reliability before practical deployment.

Despite significant progress in healthcare cybersecurity research, many existing systems continue to experience limitations related to scalability, computational cost, interoperability, incomplete attack resistance, and insufficient preparation for quantum-era threats. Some authentication frameworks prioritize security but introduce excessive computational overhead, making them unsuitable for real-time healthcare applications. Others focus on efficiency while sacrificing long-term security resilience. Consequently, there remains a strong need for lightweight, scalable, secure, and post-quantum authentication mechanisms specifically designed for cloud-based healthcare environments. The proposed work attempts to address these research gaps by integrating multifactor authentication, post-quantum security, cloud-enabled healthcare architecture, and formal verification within a unified authentication framework.

**Proposed System Architecture**

The proposed healthcare management system follows a cloud-based architecture designed to provide secure, scalable, and centralized healthcare services. The architecture consists of six major modules: Admin, Hospital, Doctor, Patient, Medical Store, and Cloud Server. Each module performs specific responsibilities within the healthcare ecosystem to ensure efficient



https://doi.org/10.63665/IJMEC.1104s.54
ISSN: 2456-4265
IJMEC 2026

management of medical data and services. The Admin module is responsible for managing the system by approving and supervising hospitals. Hospitals manage doctor registrations, billing operations, and healthcare administration. Doctors interact with patients by accessing medical reports, providing consultations, issuing prescriptions, and maintaining communication channels. Patients can upload medical reports, consult doctors, receive prescriptions, and perform online payments. The Medical Store module manages medicine inventory and medicine-related transactions. The Cloud Server acts as the central storage platform that securely stores, processes, and retrieves patient information. This architecture supports secure communication, role-based access control, centralized data management, scalability, and reliable healthcare service delivery.

**Authentication Methodology and Modules**

The proposed system adopts a structured operational methodology to ensure secure authentication and controlled access across all healthcare modules. The Admin module manages hospital registration and approval processes, ensuring that only authorized hospitals participate in the system. The Hospital module handles doctor registrations, patient bill management, and administrative healthcare operations. The Doctor module enables doctors to securely access patient reports, send digital prescriptions, provide medical consultations, and communicate with patients through chat functionality. The Patient module allows users to upload medical reports, interact with doctors, access prescriptions, and make online payments securely. The Medical Store module manages medicine availability, inventory tracking, and prescription-related medicine services. The Cloud Server module securely stores and retrieves healthcare data while maintaining confidentiality, integrity, and privacy protection. The system employs secure login procedures and controlled access mechanisms to ensure that only authenticated users can access authorized services and information.

Post-Quantum Fuzzy Commitment (PQFC) Algorithm

The proposed project introduces the Post-Quantum Fuzzy Commitment (PQFC) algorithm as the core authentication mechanism for protecting healthcare data and user identities. The PQFC scheme combines biometric authentication with post-quantum cryptographic techniques to establish secure and noise-tolerant authentication. The algorithm is represented by the expression:

C = B \oplus ECC(K)

where **B** represents the biometric feature vector, **K** denotes the cryptographic key, **ECC(K)** refers to the error-correcting encoded key, and **C** represents the generated commitment value. The algorithm securely binds biometric information with cryptographic security mechanisms, enabling reliable authentication even when minor biometric variations occur during user verification. By integrating post-quantum cryptography, the PQFC scheme strengthens protection against future quantum computing attacks while preserving user privacy, authentication reliability, and secure access control within cloud-based healthcare environments.

**Comparison with Existing Algorithms**

The proposed Post-Quantum Fuzzy Commitment scheme is compared with existing traditional cryptographic approaches and quantum-related algorithms such as Shor's Algorithm. Conventional cryptographic systems, including RSA and Elliptic Curve Cryptography (ECC), rely heavily on mathematical factorization and discrete logarithm problems for security. However, Shor's Algorithm demonstrates that sufficiently powerful quantum computers can efficiently solve these mathematical problems, making traditional cryptographic approaches vulnerable to quantum attacks. Although current quantum systems still face practical limitations such as hardware constraints, noise, and high error rates, future advancements may significantly threaten existing security infrastructures. The proposed PQFC scheme addresses these concerns by adopting lattice-based post-quantum security principles combined with biometric authentication, making it more resilient, secure, and suitable for next-generation healthcare systems that require long-term protection against emerging computational threats.

**System Design and UML Diagrams**

The software engineering design of the proposed healthcare system is developed using multiple UML diagrams to clearly represent system structure, workflows, and communication patterns. The Use Case Diagram illustrates interactions between users and system functionalities, defining how different stakeholders access healthcare services. The Class Diagram describes the relationships among system classes, attributes, and methods used in the application. The Sequence Diagram represents the communication flow between system entities during different operational processes. The Activity Diagram models workflow sequences and decision-making processes within healthcare operations. The Deployment Diagram defines the physical arrangement of software components, cloud infrastructure, and communication networks. The Entity Relationship (ER) Diagram illustrates relationships among database entities and data management processes. Together, these diagrams support a modular, maintainable, scalable, and cloud-oriented software architecture.

**Requirements, Tools, and Conclusion**

The proposed healthcare management system is developed using modern hardware and software technologies to support secure and efficient operation. The implementation environment includes Java EE technologies such as JSP and Servlets for application development, MySQL for database management, Apache Tomcat as the web server, Windows operating system as the deployment platform, and Eclipse IDE for software development and testing. The functional requirements of the system include secure user login, medical report uploading, live messaging between doctors and patients, online payment processing, and cloud-based data



https://doi.org/10.63665/IJMEC.1104s.54
ISSN: 2456-4265
IJMEC 2026

storage. Non-functional requirements emphasize security, scalability, reliability, usability, and performance optimization. The project concludes that the proposed healthcare management system successfully achieves secure cloud storage, post-quantum authentication, efficient patient–doctor communication, real-time healthcare management, and strong resistance against modern cybersecurity threats. The study demonstrates that post-quantum multifactor authentication provides a secure, scalable, and future-ready solution for cloud-assisted healthcare systems.

**REFERENCES**

[1] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018.

[2] D. He, N. Kumar, J. H. Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," *IEEE Transactions on Consumer Electronics*, vol. 60, no. 1, pp. 30–37, Feb. 2014.

[3] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.

[4] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[5] B. Blanchet, "Automatic verification of cryptographic protocols: A tutorial," *Foundations and Trends in Privacy and Security*, vol. 1, no. 1–2, pp. 1–135, 2016.

[6] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS)*, Santa Fe, NM, USA, 1994, pp. 124–134.

[7] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.

[8] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization," Gaithersburg, MD, USA, 2024.

[9] A. A. Abd El-Latif, B. Abd-El-Atti, M. Amin, and A. I. Eldesouky, "Quantum inspired blockchain-based cybersecurity framework for healthcare systems," *IEEE Access*, vol. 8, pp. 42468–42475, 2020.

[10] H. Yang, Y. Zhang, and J. Zhou, "Secure authentication protocols for cloud-assisted healthcare systems: A survey," *Journal of Network and Computer Applications*, vol. 173, Jan. 2021.

[11] A. K. Das, M. Wazid, and N. Kumar, "Secure and efficient anonymous authentication scheme for cloud-assisted healthcare applications," *Computer Networks*, vol. 140, pp. 235–248, Jul. 2018.

[12] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1–17, 2008.



https://doi.org/10.63665/IJMEC.1104s.54
ISSN: 2456-4265
IJMEC 2026