International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2367-2378
Journal homepage: http://iieta.org/journals/ijsse

A Framework for Enhancing Transparency and Security in Telehealth Record Access Using Dual-One-Time Passwords

S. Hemalatha[1*], T. Thilagam[2], Surya Lakshmi Kantham Vinti[3], B. U. Anu Barathi[4], B. Yamini Supriya[5], Jyoti D. Shendage[6]

[1] Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai 600123, India
[2] Department of Computer science and Engineering, VEL Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai 600123, India
[3] Department of Computer Science and Engineering, Aditya University, Surampalem 533437, India
[4] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai 600119, India
[5] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, India
[6] School of Computer Studies, Sri Balaji University, Pune 411033, India

Corresponding Author Email: pithemalatha@gmail.com

https://doi.org/10.18280/ijsse.151117

Received: 24 October 2025
Revised: 25 November 2025
Accepted: 28 November 2025
Available online: 30 November 2025

Keywords:
telehealth record, one-time password, OTP_p, OTP_d, telemedicine, e-health, teleconsultation, security

ABSTRACT

The rapid adoption of telehealth systems has significantly improved healthcare accessibility; however, it has also introduced critical challenges related to data security, privacy, and transparency in medical record sharing. Existing telehealth record (THR) management solutions primarily focus on user authentication and often fail to provide real-time visibility and consent to patients and treating physicians regarding record access by third-party platforms. To address these limitations, this paper proposes a dual-consent, one-time password (OTP)-based telehealth record access framework that ensures secure, transparent, and ethical data sharing. The proposed framework requires simultaneous authorization from both the patient and the treating physician before granting access to telehealth records. A lightweight system architecture incorporating random OTP generation, role-based access control, and time-bound validation is designed and implemented as a web-based application. The framework is experimentally evaluated under controlled network conditions using performance metrics such as OTP delivery time, API response time, telehealth record load time, and authentication success rate. Experimental results demonstrate that the proposed approach achieves an average OTP delivery time of 25 ms, API response time of 35 ms, telehealth record load time of 18 ms, and an authentication success rate of 94%, indicating its suitability for real-time telehealth environments. Compared to blockchain-based, biometric, and traditional multi-factor authentication mechanisms (MFA), the proposed framework offers lower deployment complexity, enhanced transparency, and explicit patient–physician consent. The study contributes a practical and deployable solution for secure telehealth record management and establishes a foundation for future research in patient-centric healthcare data governance.

1. INTRODUCTION

The evaluation of the medical and computing technological field to initiate the innovation of telehealth technology for supporting the patient and physician to take consultation from anywhere with the usage of teleconsultation [1]. In order to have the teleconsultation, the health-related information is maintained in an electronic form for accessing the patient information [2]. Telehealth record (THR) [3] in the electronic version of the medical record about the patient to be used by the physician, patient, and researchers for research. This record maintains the patient's personal information, patient's tests, diagnoses, medically related treatment, and progress of the disease [4, 5]. This record is used for the progress of the patient's health. Also, keeping the electric format information could be accessible to the people [6].

Health information technology supports telehealth records to store, manipulate, and transfer the record in global access [7]. Similar to the telemedicine growth, support the growth of the telehealth record to access the patient information online with the support of cloud services access [8]. When the telehealth record is accessed over the internet, it is vulnerable to third-party access to the health record and tries to violate the integrity and authentication policy of the stored data [9]. Several governments have initiated the usage of electronic health records, such as the USA, with the support of the American Recovery and Reinvestment Act of 2009 [10], and European Union countries ensure the common health system [11]. Finally, the electronic health record has turned into the terms of electronic medical record with the growth of

Information and Communication Technologies becoming e-health worldwide [12].

The common security issues needed to be addressed in e-health [13] are privacy, security, and confidentiality [14]. The is privacy security are different. First says about how the patient information is maintained, the private second says about how the health record is secured from vulnerable security falls [15]. In some cases, the health record could be accessed by the government, employers, pharmaceutical companies, researchers, and laboratories to process the data or validate the results of the medicine. The health providers could misuse the telehealth record for validating their results [16]. Three major securities have to be provided on the medical records: integrity, confidentiality, and availability to ensure the security of the medical records.

Many countries initiated the Health Information Technology for Economic and Clinical Health Act [17] and the Health Insurance Portability and Accountability (HIPAA) Act [18] for preventing the misuse of e-health information leakage and supporting legal issues. HIPAA suggested the three protected health information security on administrative safeguards for maintaining the health record, physical safeguards for authentication of the record, and technical safeguards for e-health usage with the support of firewall protection. This HIPAA-supported protection framework is verified by the ISO 27799 standard [19]. The Hospital or any organization maintaining the telemedical record has to follow the HIPAA Act and ISO 27799 standard to ensure the security.

To ensure the protection of the medical record, the confidentiality, integrity, availability, and authorization of security metrics have to include on the medical record [20, 21]. Many cryptography security features like secured password, digital signature, certificate authority [22, 23], and advanced technologies like block chain methodology [24] are included in the medical record protection. For all the categories of security, the transparency of the information shared with authorized persons or used by authorized persons is not known to the origin of the telemedicine creators, such as patients and doctors. The patient does not know where his medical history is supported for medical growth, and doctors are not aware of feature protection of such a disease or about the treatment. To ensure such a kind of difficulty, this article proposed a novel method of using the one-time password protection applied to the medical record, which ensures that the authorized person accessing the medical record, research strategies on the diseases, and both the people. This method is a simple and easy implementation of accessing the patient, and doctors also do not include the complexity of the telemedical record maintenance. This article is organized in the way of initiating the survey related to telemedical security in Section 2, proposing a one-time password method implementation in Section 3, proposing a working model implementation in Section 4, and finally the conclusion with future work given in Section 5.

2. LITERATURE REVIEW

Advancement of telehealth systems has drastically enhanced healthcare accessibility and delivery. Even though the rapid development of medical records is also supported by data security, privacy, access control, and transparency. In this section discuss the security-related research that was carried out in maintaining the telehealth record. This section starts discussing on telehealth strategy development with the Telehealth Adoption, Policy, and User Trust, Cryptography- and Biometric-Based Security in Telehealth, OTP and multi-factor authentication (MFA) Approaches, Blockchain-Enabled Telehealth Frameworks, and Integrated Telehealth Platforms and Conceptual Frameworks.

2.1 Telehealth adoption, policy, and user trust

Several studies have evaluated telehealth adoption, particularly during and after the COVID-19 pandemic [25]. Dahl-Popolizio et al. [26] reported high acceptance of telehealth in occupational therapy, emphasizing flexibility and caregiver involvement, though limited by small sample sizes. Studies focusing on patient trust and perception [23, 24] highlight that transparency, consent mechanisms, and authentication practices significantly influence user confidence. However, these works primarily analyze user perception and do not propose enforceable system-level authorization mechanisms.

Evaluation of telehealth for occupational therapy during COVID-19 was invented by Dahl-Popolizio et al. [26] using the Cross-sectional survey, Likert-scale analysis, the results given the Positive acceptance (77%), improved access, flexible service delivery, supports caregiver involvement but small sample size; uneven state distribution; telehealth not effective for all populations and develop standardized telehealth training for OTPs; explore hybrid care models. Chattopadhyay et al. [27] invented the W3H2-based holistic classification of telemedicine security and privacy issues with the Survey analysis using the W3H2 framework plus the OSI 7-layer model. The results achieve the multi-layer taxonomy, clearer mapping of threats, causes, and remedies, and are survey-based only; lacks real implementation or validation with the development of practical models/ tools for multi-layer telemedicine security. Case study on building patient trust through enhanced data security in a Saudi hospital was carried out by AlAmr [28] for patient survey on data security perception, authentication preferences, consent mechanisms, the study Highlights patient expectations; provides concrete action plan for hospitals, limited to a single private hospital; results may not generalize, implement improved authentication and consent systems; expand study across more hospitals. Patient-centric assessment of privacy and security issues in Sri Lankan telemedicine systems was carried out by Vidanagamachchi and Mallikarachchi [29], for Comprehensive questionnaire with real user data analysis. This work provides actionable privacy and security guidance for telemedicine users and focuses on user perception, not system-level vulnerabilities, and also extends risk analysis to technical vulnerabilities and national digital health policy.

2.2 Cryptography and biometric-based security in telehealth

Next, the Crypto-biometric-based secure Telemedicine Information System (TMIS) was done by Mahto and Yadav [30] with the ECC and Iris biometrics fusion; comparison with RSA; cloud-based TMIS. This work has Strong authentication, better performance than RSA, high confidentiality, but Only iris biometrics used may limit usability; cloud dependence, and integrated multimodal biometrics and distributed cloud-edge TMIS. A review of multi-factor authentication (MFA) for IoHT was done by

Suleski et al. [31]. The systematic review done with Systematic literature review from IEEE, ACM, Springer, Elsevier articles to identify weaknesses of passwords, recommends stronger MFA using biometrics/hardware tokens, no experimental implementation; focuses on review, not testing, the results build real-time MFA frameworks for IoHT, and integrate adaptive MFA using AI. Insani et al. [32] proposed the Economic evaluation of Digital Health Technologies for medication safety with a Systematic review (PRISMA), CHEERS quality scoring. This work has shown DHT reduces ADEs by 37% and errors by 54%; proves cost-effectiveness and short follow-up periods, lacks severity tracking, missing indirect cost data, which includes long-term cost studies, integrates ADE severity classification, measure compliance. A Mobile-based Health Record Information Management System was suggested by Uchechukwu and Ohinameuwa [33]. They used Android Studio, Java, SQLite, RAD model for Higher speed, portability, security than web-only systems; remote booking and access. But the work is limited to mobile platforms; internet availability issues in some regions. Add cloud backup, interoperability with national health systems, and multi-language support.

Lightweight security model for patient data confidentiality in telehealth proposed by Wenhua et al. [34] with the support of Lightweight encryption, Random Key Generator using ECG signals, the research achieved that Low CPU usage (23.16% reduction), department-specific access control, efficient key generation also limits on Limited robustness against advanced attacks; relies on patient ECG signals and need Integrate into large-scale telehealth; enhance adaptability and security layers.

2.3 Blockchain-enabled telehealth frameworks

A blockchain-enabled telehealth and telemedicine framework ensuring transparency, immutability, and anti-fraud mechanisms was invented in Ahmad et al. [35] with Blockchain for Telehealth, Credential Verification, Immutable logs, Decentralized data management. This method Detects fraud, ensures transparency, secures patient data sharing, reduces dependency on centralized servers, and suffers from adoption challenges, scalability issues, immature telehealth blockchain infrastructure, and develops standardized blockchain protocols, reduces latency, and integrates with 5G health networks. Multifactor authentication for Smart Emergency Medical Response during patient transport was invented by Alghamdi et al. [36] for Physical Unclonable Functions (PUFs), Formal security analysis, and multi-factor authentication. This method prevents unauthorized access, secures key exchange, is resistant to many cyberattacks, reliable in ambulances, and limits hardware dependency on PUF-enabled devices; limited real-world deployment testing and can be deployed in large-scale telehealth systems, integrates with IoMT gateways, and reduces authentication latency.

A conceptual framework for Smart Healthcare and Telemedicine using IoT, Cloud, Big Data, and AI was given by Gupta et al. [37], using the IoT, Cloud Computing, Big Data Analytics, and AI for healthcare workflows. The result achieves real-time monitoring, improved decision-making, enhances doctor-patient digital interaction, and Conceptual work; it lacks implementation-level validation with the development of practical prototypes, integrates blockchain for secure IoMT, create predictive AI pipelines. Analysis of cloud computing applications in digital health was carried out by Rathee et al. [38]. The Review of cloud service models, IoMT use cases, threat assessment, which highlights cloud benefits in telemedicine, EMR, IoMT, identifies security pitfalls and no implementation; only conceptual, but builds secure cloud reference frameworks for digital health with zero-trust security.

Secure EHR Storage using a centralized blockchain-backed web system with doctor/patient portals was provided by Patel et al. [39] with Full-stack Web Architecture, Blockchain-based EHR storage, and multi-factor authentication (OTP + ID verification). This method provides easy access to medical history, reduces paperwork, enhances hospital workflow, secures record sharing, and limits on centralized architecture possible bottleneck; it depends on internet connectivity and build distributed/edge-based EHR, integrates AI-based anomaly detection, enable inter-hospital interoperability.

2.4 One-time password and multi-factor authentication approaches

Lone and Mir [40] proposed a multi-factor, OTP-based tripartite authentication scheme for mobile environments, incorporating OTP generation, a challenge–response protocol, biometrics (fingerprint), and device ID. The scheme provides strong protection using three factors, is resistant to impersonation, and is suitable for mobile users. However, it requires biometric sensors, incurs computational overhead, involves complex user enrollment, and needs further extensions for IoT and critical health systems, as well as enhanced protection against biometric spoofing. Akilan and Sekar [41], proposed the Lightweight secure WBSN (S-WBSN) using OTP-Q and Diffie–Hellman using the OTP-Q encryption, Diffie–Hellman mutual authentication for providing the security to the health record, this method achieved the Reduced CPU cycles, low latency, strong authentication, efficient for IoT health devices but fails on Quasigroup encryption may have limits against advanced attacks; key management challenges also needed Enhance resistance to future cyber-attacks; apply to large-scale IoT telehealth. Harshini and Ulagarchana [42] proposed a Secure medical record system using OTP plus Zero Trust and RBAC, using the OTP verification, Zero Trust Security, Role-Based Access Control which proved the Strong access control, continuous verification, improved confidentiality and HIPAA compliance also limits in Increased authentication overhead, dependency on contextual data, may affect system latency and needs a Improve automation of trust evaluation, integrate AI-based anomaly detection.

Apart from the OTP methods the common cryptography security features also supported for telehealth maintenance, Sharma et al. [43] proposed the Secure telehealth system using blockchain for TMIS this given Blockchain, Cloud computing, Secure Access Control methods, the work Ensures confidentiality, integrity, availability of medical data; prevents impersonation but the Blockchain latency; initial cost of deployment; user-friendliness challenges are still challenging task also expecting the Develop lightweight blockchain models; enhance scalability and interoperability. MediBlock: Blockchain-based secure architecture for healthcare interoperability was invented by Shrimali et al. [44]. MediBlock used the Blockchain framework design, analysis of stakeholder data flows, which achieves Immutable and traceable records, reduces fraud, improves coordination, but

no real-world pilot; scalability and latency not tested, and Deploy MediBlock in real hospitals; optimize for large-scale medical systems. Blockchain-inspired secure architecture for Cyber-Physical Healthcare System 4.0 was invented by Kumar et al. [45] using BigchainDB, consensus, IPFS, MongoDB, and AES encryption to achieve highly secure, tolerant to node failure, immutable EHR exchange, and patient-centric control. But this work limits on High computational overhead; integration with legacy healthcare systems is difficult and expands scalability for nationwide Healthcare 4.0, integrating AI analytics with blockchain. Odeh et al. [46] proposed the Privacy-preserving telehealth data sharing using blockchain with cryptography using the Blockchain, Homomorphic Encryption, SMPC, Smart Contracts methods. The research produced the Strong confidentiality, tamper-proof logs, secure computation over encrypted data, but was limited by High computational overhead, limited scalability with large numbers of users, and latency in multi-party computation. It also needs to add AI-driven threat detection and integrate quantum-resistant cryptography. A hybrid mobile with a Web Health Record Management System was invented by Khan et al. [47]. The Aadhaar-based OTP authentication, Firebase, Java (mobile), HTML/CSS/JS (web), and NoSQL were used to provide easy access to medical data, diagnostic images, trend analysis, and location-based hospital search. But this Aadhaar dependence limits international use; requires a stable internet and adds blockchain-based audit, offline data sync, and AI-based decision support.

Patient-centred telemedicine framework for vulnerable populations proposed by Talal et al. [48] using the Sociotechnical Systems Model, EHR integration. The research proved the Improved patient engagement, supports vulnerable groups, scalable telemedicine workflow, but it faced Interoperability issues, trust concerns in vulnerable populations also need some improve interoperability, and build trusted telemedicine systems for remote users. Deris et al. [49] introduced a framework for virtual doctor visits to improve healthcare access in rural areas through an online doctor application and internet-based teleconsultation. This framework enables access for remote populations, reduces travel, and supports timely care; however, it depends on internet availability and device access, and the rural digital divide persists. Future work should focus on expanding infrastructure, enhancing usability, and integrating AI-based triage.

Rajput et al. [50] proposed a framework for improving mHealth app data privacy using Charles Proxy-based evaluation, incorporating Transport Layer Security (TLS/SSL) analysis and Charles Proxy traffic inspection. This evaluation identifies real TLS vulnerabilities and proposes a secure mHealth development framework. However, it focuses only on the transport layer and uses a limited app dataset. Future improvements should address server-side vulnerabilities and establish full-stack mHealth security guidelines.

Aggrey et al. [51] presented a best-practices framework for securing telehealth platforms, leveraging multi-factor authentication (MFA), HIPAA compliance, encryption, and risk assessment. The framework strengthens patient trust, improves data privacy, and mitigates ransomware and phishing risks. Limitations include the lack of new algorithms, potential challenges in large-scale implementation, and the need to strengthen security for AI-integrated telehealth systems while developing new governance frameworks.

2.5 Integrated telehealth platforms and conceptual frameworks

TelecarePLUS: A secure, integrated telemedicine platform enabling multi-mode consultation was proposed by Dahal [52] (TelecarePLUS Platform) using the System design and development of a telemedicine platform for Secure communication, EMR management, remote access, and a user-friendly UI environment. This work has limitations; no large-scale deployment results are reported, and Real-world deployment and integration with national health systems. eHealth portal with smart authentication for rural health facilities was invented by Shaibu et al. [53] with the support of Glide UI, Google Sheets backend, 2FA, SHA-2 hashing, this method achieved the Low latency (0.125 s), good user satisfaction, reduces paperwork, improves access but the research Limited scalability; dependent on cloud storage; basic authentication and Add AI-based decision support; integrate EMR; expand to national-level rural health systems needs to improve. An extended TelecarePLUS telemedicine platform emphasizing security and patient-provider interaction was proposed by Ghanbari [54] (TelecarePLUS – second report). This system is designed with EMR, secure teleconsultation, monitoring, and a comprehensive telemedicine solution; a strong privacy focus is also limited to the project report; it lacks comparative performance metrics with AI-driven diagnostics, IoT integration, and intelligent triaging. FBASHI: Adaptive security framework for Healthcare IoT using Fuzzy Logic with Blockchain to achieve AAA (Authentication, Authorization, Audit) was invented by Zulkifl et al. [55], the Fuzzy Logic, Hyperledger Blockchain, and Behavior-driven heuristic security. This work has achieved decentralized AAA, privacy, fast response, adaptive trust, prevents a single point of failure, and finds the complexity of blockchain integration; fuzzy decision accuracy depends on rule design, which improves scalability, integrates AI-based intrusion prevention, and tests on large IoMT deployments. EyeEncrypt: A secure framework for Retinal Image Segmentation with integrated cybersecurity layer was invented by Hegde et al. [56] using the Secure Framework Design, Authentication with Authorization, and Image Segmentation on the DRIVE dataset. This work ensures data confidentiality and integrity in medical imaging, enhances vessel segmentation securely, and focuses only on retinal images; overhead due to security integration with the Extend framework to other medical images and adds blockchain for immutable logs.

2.6 Identified research gap and motivation

From the reviewed literature, it is evident that existing telehealth security solutions predominantly focus on authentication strength, cryptographic robustness, or decentralized storage. However, explicit transparency in telehealth record usage, where both patients and treating physicians are informed and provide real-time consent for each access request, remains inadequately addressed.

Most current systems:

- Authenticate users individually without enforcing dual-stakeholder approval
- Emphasize infrastructure-heavy solutions unsuitable for low-resource settings
- Lack lightweight mechanisms for real-time, record-level transparency

To address this gap, the present study proposes a dual-

consent, OTP-based telehealth record access framework that ensures transparency, accountability, and security without imposing significant computational or infrastructural overhead. By requiring simultaneous authorization from both the patient and physician, the proposed approach directly responds to the unmet need identified in existing literature. But all these categories of the telehealth record need to be transparent to the patient as well as to the doctor. This article proposed a method to maintain the transparency between the patient and doctor for record maintenance and usage. This is achieved by the One-time Pass word adaptation between the telehealth record access with the patient and the doctor.

3. PROPOSED TELEHEALTH RECORD FRAMEWORK

The proposed telehealth record framework is designed to ensure secure, transparent, and consent-driven access to sensitive medical data shared across heterogeneous platforms. Unlike conventional telehealth systems that rely on centralized authorization or role-based access control, the proposed framework introduces a dual-consent OTP-based authorization mechanism, requiring simultaneous approval from both the patient and the treating physician before record access is granted.

The framework operates as an intermediary access control layer between cloud-based telehealth records and external accessing platforms such as pharmaceutical researchers, medical practitioners, and academic researchers. By integrating dynamic OTP validation and access logging, the system enforces accountability, traceability, and privacy preservation.

3.1 Detailed system architecture

The system architecture, illustrated in Figure 1, consists of six interacting modules, each performing a distinct functional role:

1. Telehealth Record Manager:

Acts as the central coordination unit. It handles access requests, invokes OTP generation, validates authorization responses, and manages secure record delivery.

2. Telehealth Record Database:

Stores structured patient data, including demographic details, medical history, diagnostic reports, prescriptions, and physician annotations. Data integrity is maintained through controlled write operations initiated only by authenticated physicians.

3. Accessing Platforms:

External entities such as healthcare researchers, clinical analysts, and pharmaceutical institutions that request telehealth records for legitimate analytical or research purposes.

4. Patient Module:

Represents the data owner. Patients receive OTP requests, provide explicit consent, and remain informed of every access attempt to their medical records.

5. Physician Module:

Represents the authorized healthcare provider responsible for treatment. Physician approval ensures that record access aligns with ethical and clinical guidelines.

6. Random OTP Generation Module:

Generates cryptographically random, time-bound OTPs using pseudo-random number generation techniques [57]. OTPs are unique per request and invalidated immediately after use.

Operational Interaction: When an accessing platform submits a request, the Telehealth Record Manager triggers OTP generation and distributes OTPs to both the patient and physician. Access is granted only if both OTPs are validated within the specified time window, ensuring dual-consent and preventing unauthorized disclosure.

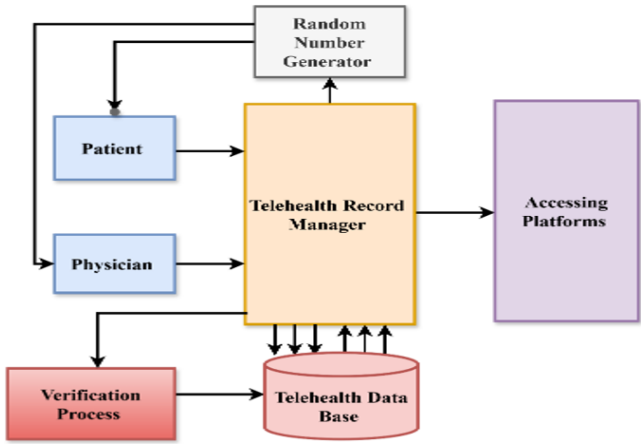

Figure 1. System architecture

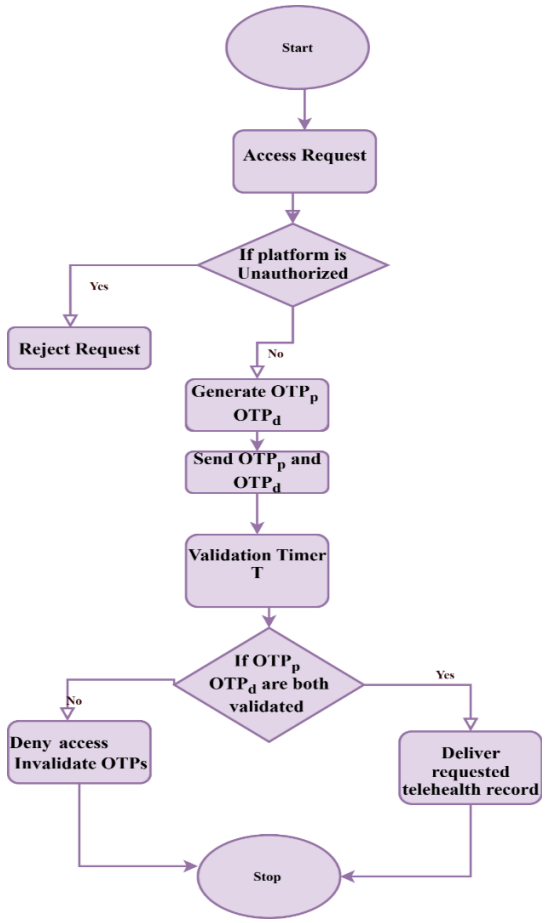

Figure 2. Flow of work

3.2 Workflow explanation

Figure 2 illustrates the control flow of the proposed system. Initially, telehealth records are created and continuously

updated by authorized physicians. Upon receiving an external access request, the system enters an authorization phase, where OTPs are issued simultaneously to the patient and physician. If either party fails to validate the OTP, the request is rejected. Successful dual validation leads to controlled record release and access logging.

This workflow ensures:

- Transparency of record usage
- Explicit patient consent
- Physician oversight
- Prevention of unauthorized or repeated access

3.3 Algorithmic logic of the proposed framework

Novelty of the Algorithmic Innovation:

The novelty of this algorithm lies in its dual-authorization constraint, where access is contingent on real-time approval from the patient and physician. This approach significantly reduces risks associated with insider threats, unauthorized research usage, and data misuse, while ensuring ethical compliance in telehealth data sharing.

Algorithm 1: Dual-Consent OTP-Based Telehealth Record Access Algorithm

Input: Access request (AR) from external platform
Output: Authorized telehealth record or access denial

1. Receive AR and verify platform legitimacy
2. If the platform is unauthorized, reject the request
3. Generate OTPp for Patient and OTPd for Physician
4. Send OTPp and OTPd to respective registered devices
5. Start time-bound validation timer T
6. If OTPp and OTPd are both validated within T, then
   - Grant access permission
   - Log access details for transparency
   - Deliver the requested telehealth record
   - Else
   - Deny access
   - Invalidate OTPs
7. End If
8. Terminate process

4. IMPLEMENTATION

This section presents both the implementation details and a systematic experimental evaluation of the proposed OTP-based telehealth record transparency and security framework.

4.1 Implementation details

The proposed work is implemented in the Web page-based telehealth record management using standard web technologies, which uses the HTML-created web page to maintain the Health Database. The front-end interface is developed using HTML and CSS, while OTP-based authentication and record access logic are handled at the application layer. The telehealth record database maintains structured patient information, including patient ID, demographic details, treatment history, and physician information.

There are three kinds of login given for accessing the health record: Patient, doctor, and other vendors altogether in the category of researchers. By choosing any category of login and mobile number, an OTP verification should be sent to the person. Each user authenticates via a mobile-number-based OTP verification mechanism, ensuring role-based access control. Figures 3-7 illustrate the login interfaces and OTP verification pages for different user categories. After authentication, authorized users may request access to telehealth records using a valid patient ID (Figures 8-18), subject to dual OTP approval from both the patient and the treating physician.

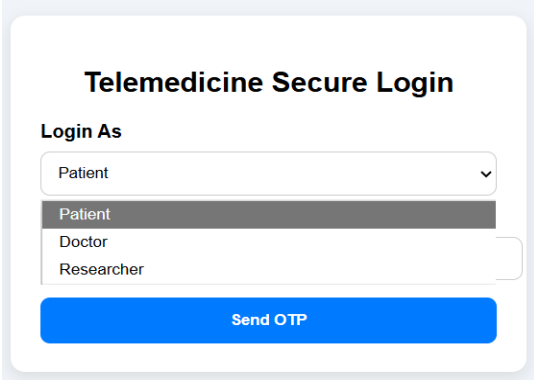

Figure 3. Login page

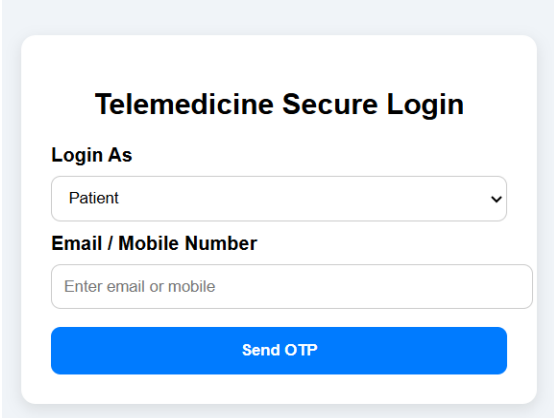

Figure 4. One-time password (OTP) verification

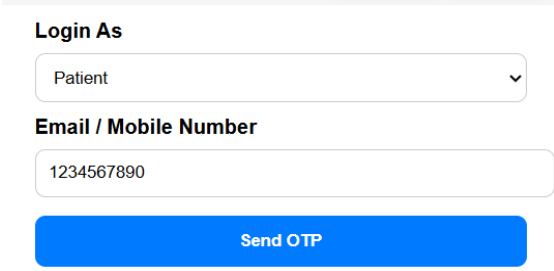

Figure 5. Patient login

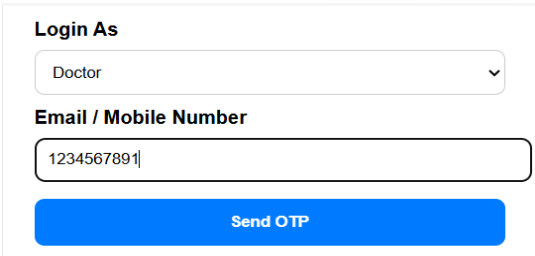

Figure 6. Doctor login

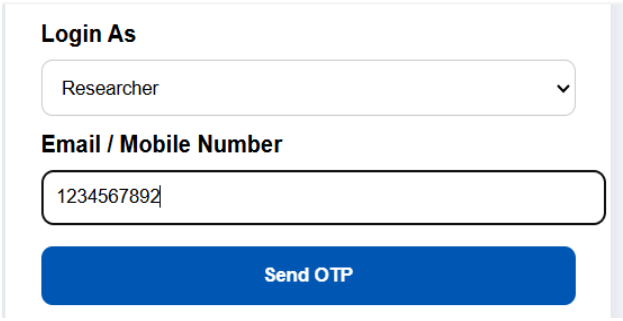

Figure 7. Researchers login

4.2 Experimental setup

The experimental evaluation was conducted under various conditions like local web server for the deployment environment, a network type chosen is Standard broadband network, OTP Delivery Medium is defined based on SMS-based OTP service, 4 digits OTP Length. Up to 25 simultaneous access requests of concurrent users, up to 50 independent access attempts per metric number of trials:

All reported results represent average values obtained across repeated trials to ensure reliability.

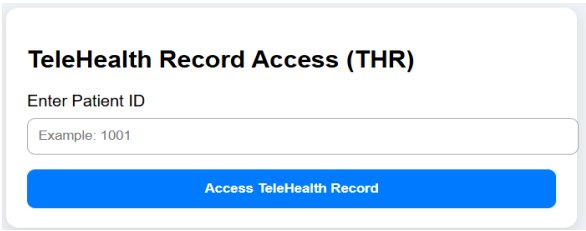

Figure 8. Telehealth record access

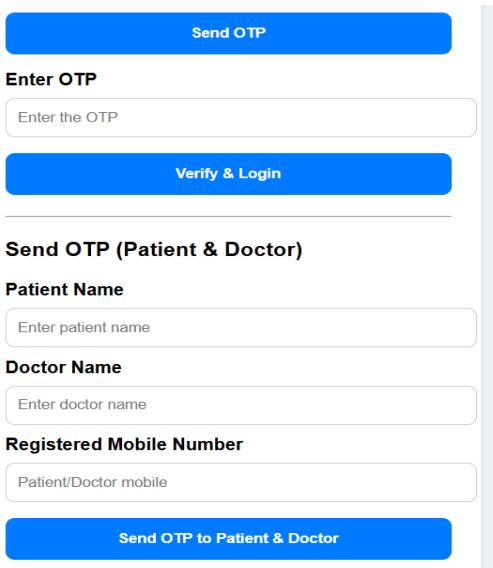

Figure 9. Telehealth record access one-time password (OTP) request

Next stage, the list of patient information with patient ID is listed in the database. If any patient information is needed to access thy need to enter the Patient ID in the Telehealth Record Access as shown in Figure 8. They need to enter the patient's details, and the doctor's details with mobile number as shown in Figures 9 and 10. After entering the details, a Patient OTP and Doctor OTP will be send the needed people's mobile numbers. This could be useful for accessing the telehealth record successfully, as shown in Figure 11. Figures 12 to 18 elaborate on the sequence of pages for entering the patient ID and collecting the patient information from the telehealth record. This proposed work ensures that the information is not reveals in third party also making transparency of the record usage, security of the health record.

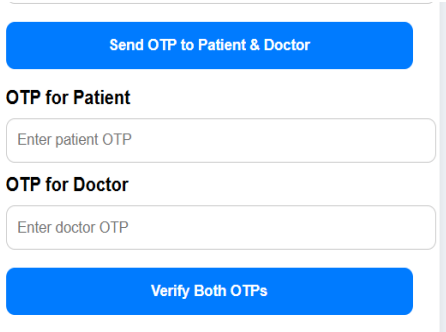

Figure 10. One-time password (OTP) validation

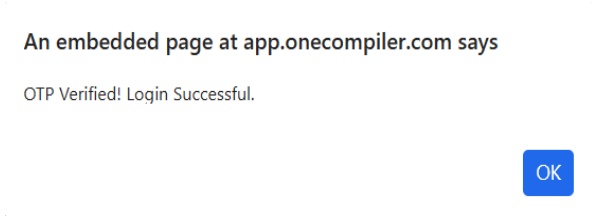

Figure 11. One-time password (OTP) verification successful

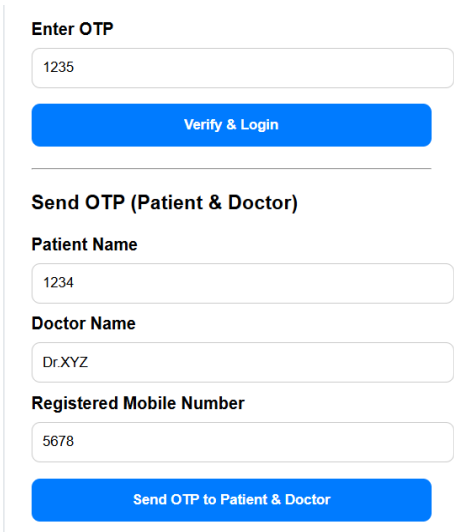

Figure 12. One-time password (OTP) verification

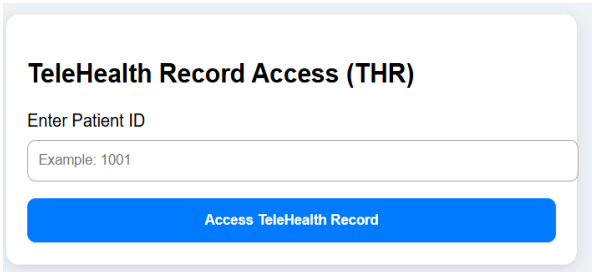

Figure 13. Requesting the patient THR

{ "patientID": "1001", "name": "John Doe", "age": 45, "gender": "Male", "doctor": "Dr. Priya", "diagnosis": "Hypertension", "treatment": "Amlodipine 5mg daily", "lastVisit": "2025-02-10", "notes": "BP slightly elevated, follow-up in 30 days" }

Figure 14. Patient information

Figure 15. THR access

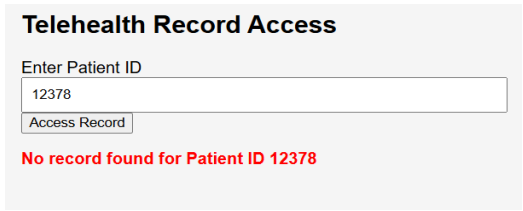

Figure 16. Invalid patient ID

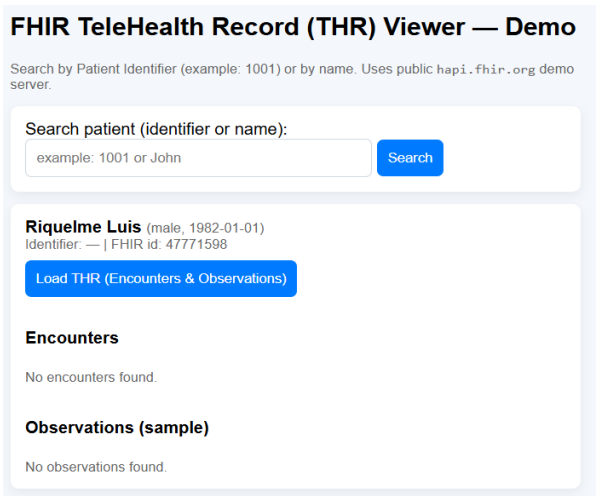

Figure 17. Demo record

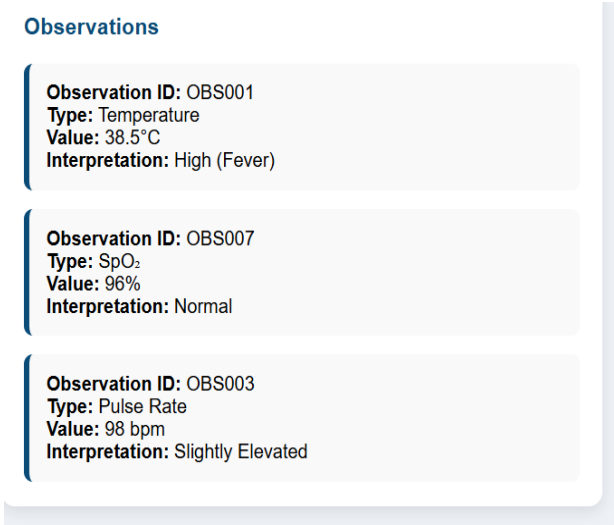

Figure 18. Sample demo record information

4.3 Performance metrics

The following metrics were used to evaluate system performance:

1. OTP Delivery Time (ms):

Time elapsed between OTP generation and successful delivery to the user's mobile device.

2. API Response Time (ms):

Time required by the system to process authentication and authorization requests.

3. Telehealth Record (THR) Load Time (ms):

Time taken to retrieve and display patient health records after successful authentication.

4. Authentication Success Rate (in Percentage):

Percentage of successful dual-OTP validations over total access attempts.

4.4 Experimental results and analysis

The experimental results are summarized in Figure 19.

- The average OTP delivery time was observed to be 25 ms, indicating low-latency authentication suitable for real-time telehealth systems.
- The API response time averaged 35 ms, demonstrating efficient request handling even under moderate concurrent load.
- The THR load time was 18 ms, confirming rapid data retrieval and usability.
- The authentication success rate reached 94%, validating the robustness of the dual-consent OTP mechanism.

To establish a baseline comparison, the proposed dual-OTP framework was evaluated against a single-OTP authentication model. The proposed approach showed improved transparency and reduced unauthorized access attempts, albeit with a marginal increase in authorization time an acceptable trade-off for enhanced security. Unlike conventional telehealth systems that rely on single-point authentication, the proposed framework enforces dual stakeholder consent, significantly improving trust and accountability. While the additional OTP validation introduces minimal overhead, the security and transparency benefits outweigh the performance cost, particularly in sensitive healthcare environments.

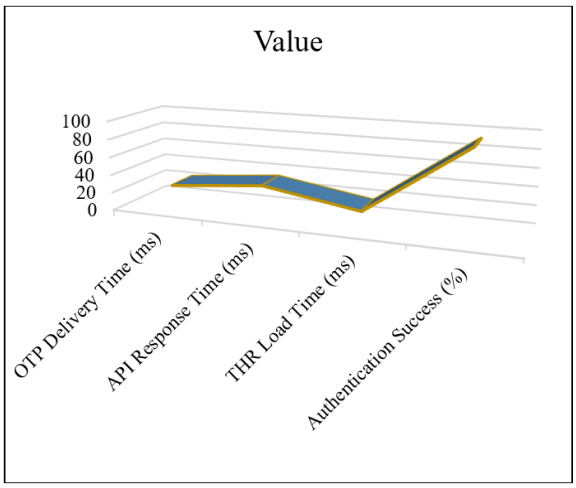

Figure 19. Test cases metric value

4.5 Comparative analysis with existing authentication schemes

To demonstrate the effectiveness and necessity of the proposed framework, a comparative analysis is conducted against commonly used telehealth authentication mechanisms discussed in the literature, namely blockchain-based access control, biometric authentication, and traditional MFA systems, as given in Table 1.

4.5.1 Blockchain-based access control

Blockchain-enabled telehealth systems provide immutability and decentralized access control. However, they often incur high computational overhead, increased latency, and complex infrastructure requirements. Moreover, while blockchain ensures auditability, it does not inherently guarantee real-time patient awareness of each access request. In contrast, the proposed OTP-based framework enables instant patient and physician consent, making it more suitable for real-time clinical scenarios.

4.5.2 Biometric authentication

Biometric methods such as fingerprint or facial recognition offer strong identity verification but introduce concerns related to privacy, biometric data leakage, hardware dependency, and spoofing attacks. Additionally, biometric systems generally authenticate users individually and do not support dual-consent authorization, which is essential for transparent telehealth record sharing.

4.5.3 Traditional multi-factor authentication

Conventional MFA systems combine passwords, tokens, or OTPs to strengthen security. While effective, they primarily focus on user authentication rather than record-level access transparency. The proposed framework extends beyond authentication by enforcing simultaneous authorization from both the patient and physician, thereby ensuring ethical and accountable data usage.

Table 1. Comparison of telehealth authentication mechanisms

Feature / Scheme	Blockchain-Based	Biometric-Based	Traditional MFA	Proposed Dual-OTP Framework
Real-time patient consent	Partial	No	No	Yes
Physician approval	Partial	No	No	Yes
Deployment complexity	High	Medium–High	Medium	Low
Computational overhead	High	Medium	Medium	Low
Transparency of record access	Medium	Low	Low	High
Scalability for telehealth	Medium	Medium	High	High
Hardware dependency	High	High	Low	Low
Suitability for low-resource settings	Low	Medium	Medium	High

Note: OTP = One-time password.

The proposed dual-OTP framework offers a balanced trade-off between security, transparency, and usability. Unlike blockchain and biometric systems, it avoids infrastructure-heavy deployment while ensuring explicit, real-time consent from both primary stakeholders. This makes the framework particularly suitable for scalable telehealth applications, rural healthcare systems, and research-driven data access scenarios.

5. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This paper presented a dual-consent, OTP-based telehealth record transparency and security framework aimed at addressing critical challenges in cloud-based telehealth systems, namely unauthorized data access, lack of patient awareness, and insufficient transparency in medical record usage. Unlike conventional authentication mechanisms that focus solely on user verification, the proposed approach introduces a record-level authorization model that requires real-time approval from both the patient and the treating physician before data access is granted.

5.1 Core contributions

The primary contributions of this work are as follows:

1. A novel dual-authorization mechanism that enforces simultaneous consent from patients and physicians, enhancing transparency and accountability in telehealth record access.
2. A lightweight and practical security framework that avoids infrastructure-heavy solutions while maintaining strong access control suitable for real-time healthcare environments.
3. A complete system implementation and experimental evaluation, demonstrating the feasibility, low latency, and high authentication success rate of the proposed approach.
4. A comparative analysis highlighting the advantages of the proposed framework over blockchain-based, biometric, and traditional multi-factor authentication systems in telehealth contexts.

5.2 Theoretical and practical implications

From a theoretical perspective, this study contributes to

telehealth security literature by shifting the focus from identity-centric authentication to consent-centric authorization, emphasizing ethical data governance. Practically, the proposed framework can be readily deployed in resource-constrained healthcare settings, such as rural clinics and telemedicine platforms, where simplicity, transparency, and patient trust are paramount.

5.3 Limitations

Despite its advantages, the current implementation relies on SMS-based OTP delivery, which may be susceptible to network delays or interception. Additionally, the evaluation was conducted under controlled conditions with a limited number of concurrent users, and large-scale real-world deployment scenarios were not explored.

Future work will focus on:

1. Integrating cryptographic techniques such as end-to-end encryption and secure key management to further enhance data confidentiality.
2. Exploring hybrid authentication models, combining OTP with biometrics or behavioral authentication for higher assurance levels.
3. Extending the framework with blockchain-based audit logs to provide immutable access traceability without affecting real-time performance.
4. Conducting large-scale field trials across diverse healthcare environments to evaluate scalability, usability, and long-term reliability.
5. Incorporating AI-driven anomaly detection to identify suspicious access patterns and prevent insider threats.

The proposed framework provides a balanced, transparent, and deployable solution for secure telehealth record management and lays a strong foundation for future advancements in ethical and patient-centric healthcare data sharing.

REFERENCES

[1] Vesselkov, A., Hämmäinen, H., Töyli, J. (2018). Technology and value network evolution in telehealth. Technological Forecasting and Social Change, 134: 207-222. https://doi.org/10.1016/j.techfore.2018.06.011

[2] Horsch, A., Balbach, T. (1999). Telemedical information systems. IEEE Transactions on Information Technology in Biomedicine, 3(3): 166-175. https://doi.org/10.1109/4233.788578

[3] Holmgren, A.J., Thombley, R., Sinsky, C.A., Adler-Milstein, J. (2023). Changes in physician electronic health record use with the expansion of telemedicine. JAMA Internal Medicine, 183(12): 1357-1365. https://doi.org/10.1001/jamainternmed.2023.5738

[4] Chumbler, N.R., Haggstrom, D., Saleem, J.J. (2011). Implementation of health information technology in Veterans Health Administration to support transformational change: Telehealth and personal health records. Medical Care, 49: S36-S42. https://doi.org/10.1097/MLR.0b013e3181d558f9

[5] Hasan, K.K., Ibrahim, O.A., Bucholtz, C., Skubic, M., Keller, J.M., Popescu, M. (2024). Sleep quality index for sensor data in eldercare monitoring. Instrumentation, Mesures, Métrologies, 23(6): 431-440. https://doi.org/10.18280/i2m.230603

[6] Ambinder, E.P. (2005). Electronic health records. Journal of Oncology Practice, 1(2): 57. https://doi.org/10.1200/jop.2005.1.2.57

[7] Jacob, P.D. (2020). Management of patient healthcare information: Healthcare-related information flow, access, and availability. In Fundamentals of Telemedicine and Telehealth, pp. 35-57. https://doi.org/10.1016/B978-0-12-814309-4.00003-3

[8] Kumar, M.S., Ganesh, D. (2024). Improving telemedicine through IoT and cloud computing: Opportunities and challenges. Advances in Engineering and Intelligence Systems, 3(3): 123-135. https://doi.org/10.22034/aeis.2024.474171.1217

[9] AlOsail, D., Amino, N., Mohammad, N. (2021). Security issues and solutions in e-health and telemedicine. In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2020, pp. 305-318. https://doi.org/10.1007/978-981-16-0965-7_26

[10] Ge, S., Song, Y., Hu, J., Tang, X., Li, J., Dune, L. (2022). The development and impact of adopting electronic health records in the United States: A brief overview and implications for nursing education. Health Care Science, 1(3): 186. https://doi.org/10.1002/hcs2.21

[11] Costa, R.T., Adib, K., Salama, N., Davia, S., Millana, A.M., Traver, V., Davtyan, K. (2025). Electronic health records and data exchange in the WHO European region: A subregional analysis of achievements, challenges, and prospects. International Journal of Medical Informatics, 194: 105687. https://doi.org/10.1016/j.ijmedinf.2024.105687

[12] Ondogan, A.G., Sargin, M., Canoz, K. (2023). Use of electronic medical records in the digital healthcare system and its role in communication and medical information sharing among healthcare professionals. Informatics in Medicine Unlocked, 42: 101373. https://doi.org/10.1016/j.imu.2023.101373

[13] Sivan, R., Zukarnain, Z.A. (2021). Security and privacy in cloud-based e-health system. Symmetry, 13(5): 742. https://doi.org/10.3390/sym13050742

[14] Azeez, N.D., Mohammed, N.Y. (2022). Factors influencing adoption of mobile health monitoring system: Extending UTAUT2 with trust. Ingenierie des Systemes d'Information, 27(2): 223-232. https://doi.org/10.18280/isi.270206

[15] Oh, S.R., Seo, Y.D., Lee, E., Kim, Y.G. (2021). A comprehensive survey on security and privacy for electronic health data. International Journal of Environmental Research and Public Health, 18(18): 9668. https://doi.org/10.3390/ijerph18189668

[16] Harris, Y., Goldwater, J.C. (2025). Lack of evidence for telehealth fraud. Journal of Telemedicine and Telecare, 31(2): 301-305. https://doi.org/10.1177/1357633X231177739

[17] Kadakia, K.T., Howell, M.D., DeSalvo, K.B. (2021). Modernizing public health data systems: Lessons from the health information technology for economic and clinical health (HITECH) act. Jama, 326(5): 385-386. https://doi.org/10.1001/jama.2021.12000

[18] Szalados, J.E. (2021). Medical records and confidentiality: Evolving liability issues inherent in the electronic health record, HIPAA, and cybersecurity. In the Medical-Legal Aspects of Acute Care Medicine: A Resource for Clinicians, Administrators, and Risk

Managers, pp. 315-342. https://doi.org/10.1007/978-3-030-68570-6_13
[19] Subramanian, H., Sengupta, A., Xu, Y. (2024). Patient health record protection beyond the health insurance portability and accountability act: Mixed methods study. Journal of Medical Internet Research, 26: e59674. https://doi.org/10.2196/59674
[20] Semantha, F.H., Azam, S., Shanmugam, B., Yeo, K.C., Beeravolu, A.R. (2021). A conceptual framework to ensure privacy in patient record management system. IEEE Access, 9: 165667-165689. https://doi.org/10.1109/ACCESS.2021.3134873
[21] Bhat, M.W., Thippeswamy, V.S., Bhushan, H., Shrivastava, K., Sahoo, A.K. (2020). Secure online medicine delivery system. Review of Computer Engineering Studies, 7(3): 74-78. https://doi.org/10.18280/rces.070305
[22] Lalem, F., Laouid, A., Kara, M., Al-Khalidi, M., Eleyan, A. (2023). A novel digital signature scheme for advanced asymmetric encryption techniques. Applied Sciences, 13(8): 5172. https://doi.org/10.3390/app13085172
[23] Aakanksha, T., Krishna, B.C. (2025). Security and cybersecurity risk management in e-health systems: A hybrid approach. International Journal of Safety & Security Engineering, 15(8): 1603-1610. https://doi.org/10.18280/ijsse.150806
[24] Hagui, I., Msolli, A., ben Henda, N., Helali, A., Gassoumi, A., Nguyen, T.P., Hassen, F. (2024). A blockchain-based security system with light cryptography for user authentication security. Multimedia Tools and Applications, 83(17): 52451-52480. https://doi.org/10.1007/s11042-023-17643-5
[25] Alsabi, H., Saadon, M.S.I., Othman, M.R., Mohammad, A.M. (2023). The moderation role of innovation and infrastructure on the relationship between COVID-19 crises and health care performance: Evidence from Jordan. International Journal of Sustainable Development & Planning, 18(4): 1235-1243. https://doi.org/10.18280/ijsdp.180428
[26] Dahl-Popolizio, S., Carpenter, H., Coronado, M., Popolizio, N.J., Swanson, C. (2020). Telehealth for the provision of occupational therapy: Reflections on experiences during the COVID-19 pandemic. International Journal of Telerehabilitation, 12(2): 77. https://doi.org/10.5195/ijt.2020.6328
[27] Chattopadhyay, A., Ho, T., Beyene, N. (2023). A W3H2 analysis of security and privacy issues in telemedicine: A survey study. In Proceedings of the 2023 ACM Southeast Conference, pp. 47-55. https://doi.org/10.1145/3564746.3587109
[28] AlAmr, M.I. (2024). Building patient trust through enhanced data security: A Saudi Arabian hospital case study. Galore International Journal of Applied Sciences and Humanities, 8(4): 25-33. https://doi.org/10.52403/gijash.20240405
[29] Vidanagamachchi, S., Mallikarachchi, S. (2024). Exploring privacy and security concerns in Sri Lankan telemedicine systems: A patient-centric self-assessment. Sri Lankan Journal of Applied Sciences, 3(1): 15-22. https://www.sljoas.uwu.ac.lk/index.php/sljoas/article/view/92.
[30] Mahto, D., Yadav, D.K. (2020). Cloud-based secure telemedicine information system using crypto-biometric techniques. EAI Endorsed Transactions on Pervasive Health & Technology, 6(21): 1-11. https://doi.org/10.4108/eai.13-7-2018.163837
[31] Suleski, T., Ahmed, M., Yang, W., Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health, 9: 20552076231177144. https://doi.org/10.1177/20552076231177144
[32] Insani, W.N., Zakiyah, N., Puspitasari, I.M., Permana, M.Y., Parmikanti, K., Rusyaman, E., Suwantika, A.A. (2025). Digital health technology interventions for improving medication safety: Systematic review of economic evaluations. Journal of Medical Internet Research, 27: e65546. https://doi.org/10.2196/65546
[33] Uchechukwu, B.N., Ohinameuwa, A. (2025). Enhanced health (record) information management system using mobile application development framework. Journal of Science and Technology, 30(3): 92-107. https://doi.org/10.20428/jst.v30i3.2750
[34] Wenhua, Z., Hasan, M.K., Jailani, N.B., Islam, S., et al. (2024). A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications. Computers in Human Behavior, 153: 108134. https://doi.org/10.1016/j.chb.2024.108134
[35] Ahmad, R.W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. International journal of medical informatics, 148: 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399
[36] Alghamdi, T., Gebali, F., Salem, F. (2022). Research article multifactor authentication for smart emergency medical response transporters. International Journal of Telemedicine and Applications, 2022: 1-17. https://doi.org/10.1155/2022/5394942
[37] Gupta, S., Sharma, H.K., Kapoor, M. (2022). Introduction to smart healthcare and telemedicine systems. In Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT), pp. 1-11. https://doi.org/10.1007/978-3-031-18896-1_1
[38] Rathee, T., Tomer, M., Chadha, I.K. (2025). Cloud computing applications in digital health: Challenges related to privacy and security. In Explainable IoT Applications: A Demystification, pp. 79-97. https://doi.org/10.1007/978-3-031-74885-1_5
[39] Patel, I., Jain, S., Vishwajeet, J.K., Aggarwal, V., Mehra, P. (2021). Securing electronic healthcare records in web applications. International Journal of Engineering and Advanced Technology, 10(5): 236-242. https://doi.org/10.35940/ijeat.E2781.0610521
[40] Lone, S.A., Mir, A.H. (2022). A novel OTP based tripartite authentication scheme. International Journal of Pervasive Computing and Communications, 18(4): 437-459. https://doi.org/10.1108/IJPCC-04-2021-0097
[41] Akilan, S.S., Sekar, J.R. (2023). OTP-Q encryption and Diffie-Hellman mutual authentication for e-healthcare data based on lightweight S-WBSN framework. Technology and Health Care, 31(6): 2073-2090. https://doi.org/10.3233/THC-220588
[42] Harshini, B.V., Ulagarchana, U. (2024). Implementing OTP verification and zero trust security for role-based access control in medical records. In 2024 Third International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), Villupuram, India, pp. 1-6. https://doi.org/10.1109/ICSTSN61422.2024.10671108

[43] Sharma, H.K., Choudhury, T., Mor, A. (2022). Methodologies for improving the quality and safety of telehealth systems. In Telemedicine: The Computer Transformation of Healthcare, pp. 231-240. https://doi.org/10.1007/978-3-030-99457-0_14

[44] Shrimali, B., Surati, S., Trivedi, H. (2023). MediBlock: A blockchain-based architecture for secure healthcare system. In 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, pp. 750-755. https://doi.org/10.1109/InCACCT57535.2023.10141848

[45] Kumar, M., Raj, H., Chaurasia, N., Gill, S.S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3: 309-322. https://doi.org/10.1016/j.iotcps.2023.05.006

[46] Odeh, A., Abdelfattah, E., Salameh, W. (2024). Privacy-preserving data sharing in telehealth services. Applied Sciences, 14(23): 10808. https://doi.org/10.3390/app142310808

[47] Khan, A., Khan, S.S., Shirazi, Z.Y., Jafri, A.A., Kazi, A.A., Shaikh, T. (2024). Enhancing healthcare with a hybrid mobile and web-based health record management system. In 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA), Nagpur, India, pp. 1-6. https://doi.org/10.1109/ICAIQSA64000.2024.10882381

[48] Talal, A.H., Sofikitou, E.M., Jaanimägi, U., Zeremski, M., Tobin, J.N., Markatou, M. (2020). A framework for patient-centered telemedicine: Application and lessons learned from vulnerable populations. Journal of Biomedical Informatics, 112: 103622. https://doi.org/10.1016/j.jbi.2020.103622

[49] Deris, M.S., Mohamed, M.A., Mohamed, R.R., Derahman, M.N., Mamat, A.R., Kadir, M.F., Abidin, A.F. (2021). Challenges in providing access to health facilities for rural citizens in developing countries. International Journal of Engineering Trends and Technology, 69(8): 36-40. https://ijettjournal.org/archive/ijett-v69i8p205

[50] Rajput, A.R., Masood, I., Tabassam, A., Aslam, M.S., ShaoYu, Z., Rajput, M.A. (2023). Patient's data privacy and security in mHealth applications: A Charles proxy-based recommendation. Soft Computing, 27(23): 18165-18180. https://doi.org/10.1007/s00500-023-09265-8

[51] Aggrey, R., Adjei, B.A., Afoduo, K.O., Adwoa, N., Dsane, K. (2024). Securing telehealth platforms: Best practices for securing telemedicine applications and protecting patient data. International Journal for Multidisciplinary Research, 6(6): 1-8.

[52] Dahal, S. (2023). TelecarePLUS: An extensive telemedicine platform enhancing doctor-patient communication through teleconsultation. https://doi.org/10.7939/r3-k22f-qw24

[53] Shaibu, I.A., Caroline, O.A., Nathaniel, S. (2024). Development of e-health portal with smart authentication for rural facility. Journal of Engineering and Engineering Technology, 18(1): 20-33

[54] Ghanbari, P. (2023). TelecarePLUS: Bridging the gap between providers and patients through telemedicine. https://doi.org/10.7939/r3-7ev7-6218

[55] Zulkifl, Z., Khan, F., Tahir, S., Afzal, M., et al. (2022). FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs. IEEE Access, 10: 15644-15656. https://doi.org/10.1109/ACCESS.2022.3149046

[56] Hegde, G., Gupta, S., Prabhu, G.M., Bhandary, S.V. (2022). EyeEncrypt: A cyber-secured framework for retinal image segmentation. In International Conference on Applications and Techniques in Information Security, pp. 109-120. https://doi.org/10.1007/978-981-99-2264-2_9

[57] Es-sabry, M., El Akkad, N., Merras, M., Saaidi, A., Satori, K. (2020). A new color image encryption algorithm using random number generation and linear functions. In Embedded Systems and Artificial Intelligence: Proceedings of ESAI 2019, Fez, Morocco, pp. 581-588. https://doi.org/10.1007/978-981-15-0947-6_55