

USE CASE/PILOT/METHODOLOGY

Enhancing Transparency and Security in Telehealth Records Using Dual One-Time Password Authorization

S. Hemalatha PhD (CSE)¹ , Kiran Mayee Adavala PhD (CSE)², Pullela S.V.V.S.R. Kumar PhD (CSE)³ , Karthi Govindharaju, PhD⁴ , N. Muthuvairavan Pillai PhD⁵ and G. Krishna Mohan PhD (CSE)⁶ 

¹Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai, Tamil Nadu, India; ²CSE (AIML), Kakatiya Institute of Technology and Science, Warangal, India; ³Department of Computer Science and Engineering, Aditya University, Surampalem, Andhra Pradesh, India; ⁴Department of CSBS, Panimalar Engineering College, Chennai, Tamil Nadu, India; ⁵Department of Computer Science and Business Systems, RMD Engineering College, Chennai, India; ⁶Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur India

DOI: <https://doi.org/10.30953/thmt.v1i1.691>

Corresponding Author: Dr. S. Hemalatha, Email: pithemalatha@gmail.com

Keywords: e-health, hypertext markup language, one-time password, teleconsultation, telehealth record, telemedicine record

Abstract

Background: Many information technologies have supported the growth of the medical field worldwide. Telehealth consultation is a rapidly developing area in healthcare that aims to optimize time utilization during patient–physician consultations. To support telehealth consultations, healthcare providers make patient records available on online platforms to review medical history and treatment progress. Accordingly, government and healthcare organizations have introduced telehealth, telemedicine, and systems for maintaining e-health records. When such data are hosted on online platforms, it becomes vulnerable to unauthorized access and potential security threats. Although security mechanisms such as firewalls and authentication controls protect telehealth records (THRs), these records are frequently accessed by government agencies, researchers, and healthcare professionals for medical analysis and research. However, authorities often do not explicitly enforce transparency regarding how and where THRs are accessed. Often, patients and treating physicians are not fully aware of external access to health records before data disclosure.

Methods: To address this limitation, the authors propose an architectural framework for THR access that uses a one-time password (OTP)-based dual-authorization mechanism to ensure both security and transparency.

Results: The proposed approach enables health record access only with the knowledge and explicit authorization of both the patient and the physician, thereby embedding transparency within the access control workflow. The system is built using web pages written in Hypertext Markup Language (HTML), and controlled testing is used to ensure the operational workflow functions.

Conclusions: Experimental results indicate:

- OTP delivery time is 15 ms,
- application programming interface (API) response time is 25 ms,
- THR load time is 15 ms, and
- authentication success rate is 97%.

Plain Language Summary

The telehealth record represents the electronic version of a patient’s medical record and is used by physicians, patients, and researchers for clinical and research purposes.

The primary security concerns in e-health systems include privacy, security, and confidentiality. Although people often use these terms interchangeably, they represent distinct aspects. To address this transparency gap the authors propose a one-time password-based dual-authorization mechanism for access to THRs. The proposed approach ensures:

- the patient and the treating physician receive notifications, and
- are involved before external entities gain access to health records.

Key Takeaways

- The proposed framework presented here enables transparent access to telehealth records.
- The overall authentication success rate is 97%.
- This framework can be extended to support wider global telehealth records, scalability, auditability, and interoperability across healthcare platforms.

The evolution of medical and computing technologies¹ has initiated significant innovation in telehealth systems, enabling patients and physicians to consult from different geographical locations through teleconsultation services.² To support teleconsultation, health-related information is stored electronically to facilitate efficient access to patient data. The telehealth record (THR)⁴ represents the electronic version of a patient's medical record and is used by physicians, patients, and researchers for clinical and research purposes. This record maintains patients' personal information, diagnostic reports, laboratory test results, medical treatments, and disease progression details.⁵ Maintaining such records in electronic format allows continuous monitoring of patient health conditions and enables authorized access from different locations.⁶

Health Information Technology supports THRs by enabling storage, manipulation, and transfer of data for global accessibility.⁷ With the growth of telemedicine, cloud-based platforms and online services increasingly provide access to THRs.⁸ However, when THRs are accessible over the Internet, they become vulnerable to unauthorized third-party access, potentially affecting the integrity and authentication policies of stored data.⁹ Several governments have promoted the adoption of electronic health records, including the United States under the American Recovery and Reinvestment Act of 2009¹⁰ and European Union initiatives supporting unified health systems.¹¹ With advancements in information and communication technologies, electronic health records have evolved into broader e-health ecosystems worldwide.¹²

The primary security concerns in e-health systems include privacy, security, and confidentiality.¹³ Although people often use these terms interchangeably, they represent distinct aspects. Privacy refers to maintaining patient information in a protected and controlled manner, while security relates to safeguarding health records against vulnerabilities and unauthorized access.¹⁴ In certain cases, government agencies, employers, pharmaceutical companies, researchers, and laboratories may access health records for data processing or validation purposes. There is also a potential risk of misuse by healthcare providers or other stakeholders.¹⁵ Therefore, medical records must ensure the core security principles of confidentiality, integrity, and availability.

Many countries have introduced regulations such as the Health Information Technology for Economic and Clinical Health (HITECH) Act¹⁶ and the Health Insurance Portability and Accountability Act (HIPAA)¹⁷ to prevent misuse and unauthorized disclosure of e-health information. HIPAA defines administrative safeguards for record management, physical safeguards for access control, and technical safeguards for secure electronic usage, including firewall protection. These protection frameworks also align with ISO 27799 standards for healthcare information security.¹⁸ Hospitals and organizations maintaining telemedical records must comply with these regulatory standards to ensure appropriate security measures.

To ensure effective protection of medical records, confidentiality, integrity, availability, and authorization mechanisms must be incorporated into the system architecture.¹⁹ Various cryptographic techniques (Table 1) such as secure passwords, digital signatures, and certificate authorities,²⁰ along with advanced approaches such as blockchain methodologies,²¹

Table 1. Comparison of telehealth record security approaches.

Feature	Blockchain-based approaches	Multi-factor authentication	Proposed OTP framework
Transparency in record access	Partial ^{35,36}	No ^{33,39}	Yes
Dual patient–doctor consent	No ^{35,37}	No ³³	Yes
Computational complexity	High ^{36,37}	Medium ³³	Low
Implementation cost	High ^{35,36}	Medium ³⁹	Low
Infrastructure requirements	Distributed/High ^{36,37}	Moderate ³³	Lightweight
Ease of deployment	Low ³⁵	Medium ³³	High

OTP: one-time password.

have been adopted to enhance medical record security. While these mechanisms strengthen authentication, encryption, and auditability, they do not explicitly enforce transparency at the human authorization level. In many situations, patients and treating physicians are not clearly informed prior to secondary usage or external access to medical records, even when access is technically authorized.

To address this transparency gap, this article proposes a one-time password (OTP)-based dual-authorization mechanism for access to THRs. The proposed approach ensures that both the patient and the treating physician receive notifications and are involved before external entities gain access to health records. Unlike conventional authentication models that primarily verify user identity,²² the proposed method embeds shared authorization within the access control workflow. This approach aims to enhance transparency and controlled authorization while maintaining implementation simplicity and avoiding the operational complexity associated with heavier distributed frameworks.

The remainder of this article is organized as follows. Section 'Literature review' presents the literature review on telehealth security, authentication models, blockchain frameworks, and recent AI-driven cybersecurity approaches. Section 'Proposed telehealth record framework' describes the proposed dual-authorization OTP-based THR framework along with its system architecture and workflow. Section 'Implementation' discusses the implementation details and performance evaluation metrics. Section 'Comparison with existing approaches' presents a comparative analysis with existing approaches. Section 'Limitations and privacy–cybersecurity considerations' discusses the limitations of the proposed framework and privacy–cybersecurity considerations. Finally, Section 'Conclusion' concludes the article and outlines

Literature Review

In this section, the authors discuss existing research related to security in THR maintenance. The review covers telehealth strategy development and policy initiatives; cryptographic adoption in telehealth applications; contributions of modern technologies; blockchain-based frameworks; OTP mechanisms for THR access; artificial intelligence-based cybersecurity models; zero-trust architectures; secure cloud frameworks; and various telehealth application domains.

The evaluation of telehealth for occupational therapy during the COVID-19 pandemic was carried out by Dahl-Popolizio et al.²³ in 2020 using a cross-sectional survey and Likert-scale analysis. The results indicated positive acceptance (77%), improved access, flexible service delivery, and enhanced caregiver involvement; however, limitations included a small sample size and limited applicability across all populations. Chattopadhyay et al.²⁴ proposed a W3H2-based holistic classification of telemedicine security and privacy issues in 2023 using survey-based analysis combined with the OSI seven-layer model. Their work provided a multi-layer taxonomy for identifying threats, causes, and mitigation strategies, though it lacked implementation-level validation.

AlAmr²⁵ examined patient trust through enhanced data security in a Saudi hospital in 2024 using patient surveys on authentication and consent mechanisms. While the study provided practical insights, it focused on a single institutional setting. Similarly, Vidanagamachchi and Mallikarachchi²⁶ assessed privacy and security concerns from a patient-centric perspective in Sri Lankan telemedicine systems in 2024. Their findings emphasized user awareness and perception; however, the study did not extensively analyze deeper system-level technical vulnerabilities.

Recent developments in 2025 further emphasize the growing importance of advanced cybersecurity in digital health environments. Insani et al.²⁷ evaluated digital health technologies for medication safety using Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology, demonstrating measurable reductions in adverse drug events and medication errors. Rathee et al.²⁸ analyzed secure cloud computing applications in digital health systems, highlighting scalability benefits along with the need for robust identity and access management mechanisms. Recent 2025 studies on AI-driven cybersecurity architectures for telehealth platforms have proposed intelligent threat detection models to enhance protection of virtual healthcare consultations.²⁹ Additionally, contemporary research on secure cloud infrastructure for healthcare systems stresses the importance of zero-trust identity verification and resilient authentication frameworks to protect electronic health records in distributed environments.³⁰ Systematic reviews of emerging cybersecurity technologies in 2025 further indicate that hybrid approaches integrating artificial intelligence, adaptive authentication, and risk-based access control can strengthen resilience against evolving cyber threats in healthcare systems.³¹

A crypto-biometric-based secure Telemedicine Information System (TMIS) was proposed by Mahto and Yadav³² in 2020, integrating elliptic curve cryptography with iris biometrics and cloud deployment. The system demonstrated strong authentication performance, though usability constraints and reliance on a single biometric modality were observed as limitations. Suleski et al.³³ reviewed multi-factor authentication (MFA) mechanisms for the Internet of Healthcare Things (IoHT) in 2022, identifying weaknesses in traditional password-based systems and recommending stronger MFA strategies, although experimental validation was not provided.

Wenhua et al.³⁴ introduced a lightweight encryption model for telehealth confidentiality in 2024 that uses electrocardiography (ECG)-based key generation, reducing central processing unit (CPU) utilization while raising concerns about scalability

and resistance to advanced attacks. Blockchain-enabled telehealth and telemedicine frameworks have also been widely investigated to ensure immutability and transparency. Ahmad et al.³⁵ proposed a blockchain-based telehealth framework in 2021 that provided secure data sharing but faced scalability and infrastructure challenges. MediBlock³⁶ and the blockchain-inspired Cyber-Physical Healthcare System architecture proposed by Mohit Kumar et al.³⁷ improved reliability and auditability, though computational overhead remained a concern. Odeh et al.³⁸ further enhanced privacy preservation using homomorphic encryption and secure multi-party computation in 2024, but latency and scalability limitations persisted.

OTP-based and MFA schemes have been extensively studied. Lone and Mir³⁹ proposed a tripartite OTP-based authentication framework that combines OTPs, biometrics, and device identifiers, thereby improving resistance to impersonation attacks at the cost of additional computational overhead. Akilan and Sekar⁴⁰ introduced a lightweight OTP-based authentication mechanism for wireless body sensor networks, focusing on reduced latency but encountering key management challenges. Harshini et al.⁴¹ integrated OTP with Zero Trust and role-based access control in 2024, strengthening access governance while increasing authentication complexity.

Hybrid and platform-based telehealth systems have also been proposed. Khan et al.⁴² developed a hybrid mobile-web health record system using OTP-based authentication, though its applicability was limited to specific national identity infrastructures. TelecarePLUS platforms^{43,44} emphasized secure teleconsultation workflows but lacked validation in large-scale deployments. Shaibu et al.⁴⁵ proposed a smart authentication portal for rural healthcare facilities, achieving low latency but limited scalability. Zulkifl et al.⁴⁶ introduced FBASHI, combining fuzzy logic with blockchain to provide decentralized authentication and auditing mechanisms, though system complexity increased. EyeEncrypt⁴⁷ focused on secure medical image processing with confidentiality and integrity support.

Despite these advancements, existing approaches primarily emphasize authentication strength, encryption robustness, blockchain immutability, or AI-driven intrusion detection. However, transparency in THR usage specifically ensuring that both patients and treating physicians are explicitly aware of and approve external access requests remains insufficiently addressed. While zero-trust and blockchain models improve auditability and verification, they do not inherently enforce dual human authorization prior to record disclosure. This identified gap motivates the proposed approach, which focuses on enhancing transparency between patients and physicians through OTP-based dual authorization during THR access.

Proposed Telehealth Record Framework

From the literature survey, it is observed that telehealth and telemedicine records are accessed by various platforms, including government sectors,¹¹ pharmaceutical researchers, physicians⁴⁸ for disease-related studies, and medical researchers¹⁷ for case study analysis. When such THRs are shared through cloud storage^{13,30} or online platforms, they become vulnerable to potential data security breaches.^{15,22} In addition, access to health record information is often not explicitly transparent to the patient and the treating physician prior to disclosure.

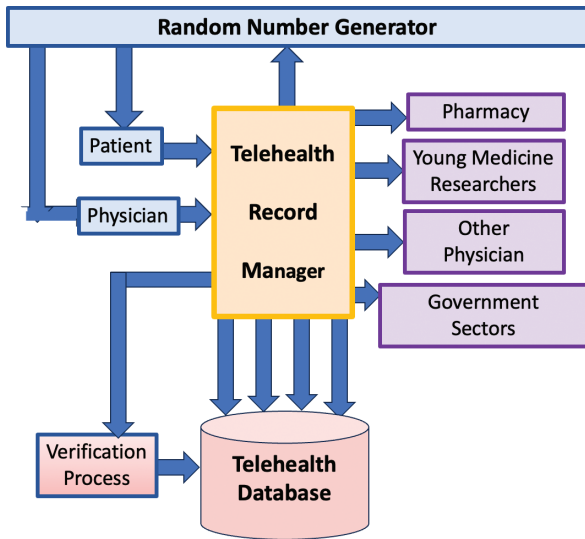


Fig. 1. System architecture.

To ensure transparency in data use while maintaining secure access to records, this article proposes a OTP-based dual-authorization mechanism for THRs. The proposed approach is integrated into the telehealth database architecture, where any access request from an external platform triggers the generation and delivery of an OTP to both the patient and the treating physician. The health record becomes available to the requesting entity only after both parties successfully verify the OTPs within a valid access session. This method maintains controlled authorization while ensuring that patients and physicians are informed about when and how THRs are accessed, including usage for research or disease analysis. The approach is intentionally lightweight and avoids the operational and computational complexity associated with more resource-intensive.

System Architecture

Figure 1 illustrates the proposed system architecture, which consists of the THR manager, THR database, various access platforms, patients and physicians, and a random OTP generation module. The THR database stores structured patient information, including personal details, medical history, treatment records, medication details, and physician information. This information is accessible only through authenticated sessions and is visible to patients and physicians to support transparency and data integrity.

Various accessing platforms, such as pharmaceutical researchers, disease specialists, and medical researchers, may request access to THRs for legitimate analytical or clinical purposes. However, such access is permitted only with the knowledge and explicit authorization of both the patient and the physician. Whenever an accessing platform submits a THR request, the THR manager activates the OTP generation module. A random number generation technique⁴⁹ is used to generate a four-digit OTP for each access request. The generated OTPs are delivered to the registered mobile numbers of both the patient and the physician. Access to the THR database is granted only after successful verification of both OTPs within the same transaction session.

Since each OTP is generated uniquely for a single access instance and is not reusable, replay or repeated access using

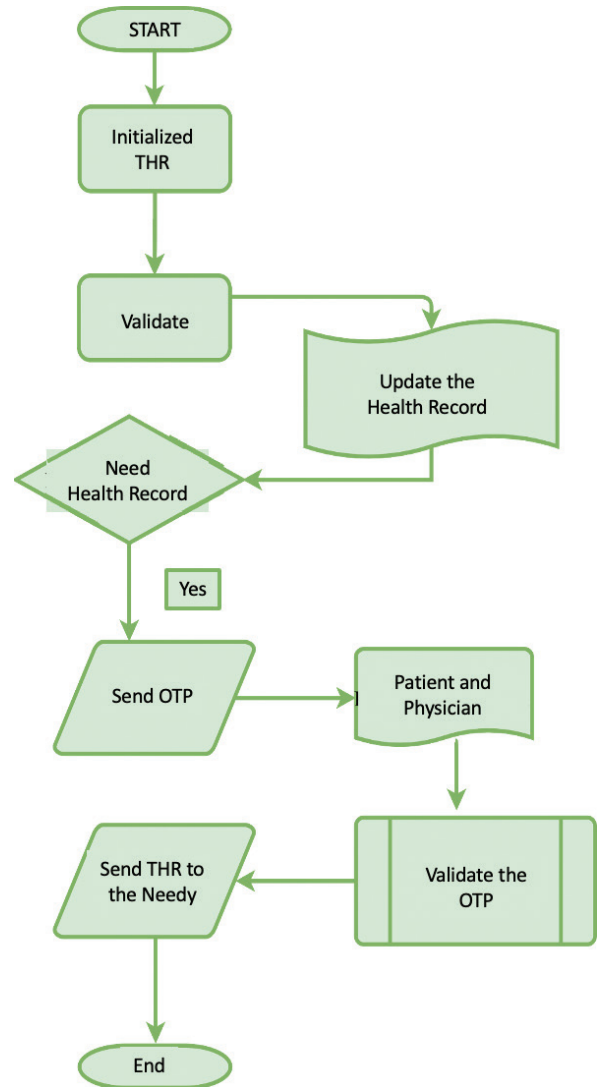


Fig. 2. Flow of work.

OTP: one-time password; THR: telehealth record.

previously issued credentials is prevented. This mechanism strengthens session-level authorization, enhances transparency in record usage, and ensures secure access for future medical analysis.

The overall operational workflow of the proposed framework for THR transparency and security is summarized in Algorithm 1 and illustrated in Fig. 2. Initially, the THR is populated with the patient's personal information, medical data, treatment details, and physician records. In the second stage, patient and physician identities are authorized using mobile-based OTP verification. THRs are updated regularly as treatments or medications are administered. When a third party requests access to a health record, OTPs are generated and sent simultaneously to both the patient and the physician. Since the OTP is valid for a single access session only, unauthorized reuse is prevented, thereby improving both security and transparency of record access.

Algorithm 1: Steps of the Proposed Framework

1. Initialize the telehealth record
2. Validate patient and physician identities using authorization access

Fig. 3. Composite login & OTP interface.

OTP: one-time password.

3. Update the health record when treatment or medication is provided
4. When an external platform requests access, send OTPs to the patient and physician
5. Confirm OTP verification
6. Validate transparency and access permissions
7. Provide telehealth record access to the requesting platform
8. End the process

Implementation

This section discusses the implementation of the proposed THR transparency and security framework. The proposed work is implemented as a web-based application using Hypertext Markup Language (HTML) to develop the user interface pages that interact with the telehealth database. Three categories of users are provided for accessing health records: patients, doctors, and other vendors categorized as researchers. By selecting the appropriate login category and providing a registered mobile number, the system generates and sends an OTP verification request to the user. After entering the received OTP, the user is authenticated and granted access to the THR system. This process ensures controlled authentication as well as secure access to the database. Figure 3 illustrates the login page, the OTP verification process, and the different login categories.

In the next stage, a list of patient information, each associated with a unique patient ID, is maintained in the telehealth database. If access to a specific patient record is required, the requesting user must enter the corresponding patient ID through the THR access interface. The user is then required to provide patient and physician details, along with the registered mobile numbers. Upon submission, OTPs are generated and sent simultaneously to both the patient and the doctor. Successful verification of both OTPs within the same access session enables authorized retrieval of the THR. A composite workflow in Fig. 4 illustrates the sequence of steps involved in patient ID validation and THR retrieval. This implementation ensures that health information is not disclosed to unauthorized third parties while supporting transparency in record usage and maintaining data security.

Fig. 4. Composite workflow screenshots of OTP verification and telehealth record access process.

OTP: one-time password; THR: telehealth record.

The performance of the proposed system was evaluated using basic performance metrics obtained from repeated access trials. The observed OTP delivery time was 15 ms, the application programming interface (API) response time was 25 ms, and the THR load time was 15 ms. Figure 5 illustrates the performance metrics of the proposed framework in terms of OTP delivery time, API response time, THR load time, and authentication success rate. The overall authentication success rate achieved was 97%.

Comparison With Existing Approaches

Several security and access control mechanisms have been proposed in the literature to protect telehealth and electronic health records, including blockchain-based frameworks, MFA systems, and zero-trust security models.^{35–37,39,41} Each approach not only provides specific advantages but also introduces limitations related to computational complexity, deployment cost, and operational overhead. The proposed OTP-based THR framework is compared with commonly adopted approaches to highlight its characteristics, particularly in terms of transparency and access authorization.

Blockchain-based approaches provide immutability and auditability of health records but often involve high computational overhead, scalability challenges, and increased deployment costs.^{35–37} The MFA-based systems enhance authentication strength by combining multiple verification factors; however, these systems primarily focus on user authentication and do not explicitly support transparency or shared

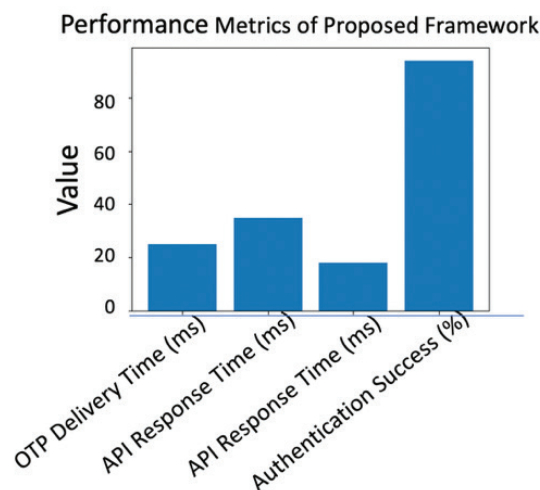


Fig. 5. Performance metric of telehealth framework.

API: application programming interface; OTP: one-time password; THR: telehealth record.

consent between patients and physicians.^{33,39} Zero-trust and role-based access control models improve continuous verification and access enforcement but may introduce additional authentication overhead and system latency.⁴¹

In contrast, the proposed OTP-based framework emphasizes dual authorization and transparency by requiring explicit approval from both the patient and the treating physician before THR access is granted. The approach is lightweight, easy to deploy, and suitable for web-based telehealth environments. It is intended to complement existing security mechanisms rather than replace advanced cryptographic or distributed security frameworks.^{50–52}

Limitations and Privacy–Cybersecurity Considerations

Limitations

Despite the advantages of the proposed THR transparency and security framework, certain limitations must be acknowledged. Firstly, the proposed OTP-based authorization mechanism depends on the availability and reliability of mobile network services. In environments with poor network connectivity, OTP delivery delays may affect timely access to THRs. Secondly, the current implementation relies on SMS-based OTP delivery, which may be vulnerable to security threats such as SIM swap attacks or message interception. Although the dual-authorization requirement involving both the patient and the physician reduces the overall risk of unauthorized access, additional secure OTP delivery channels could further enhance system robustness.

Thirdly, the proposed framework has been evaluated using a web-based prototype and limited test scenarios. It has not yet been validated in large-scale hospital environments or nationwide telehealth systems, where higher user volumes and complex workflows may introduce scalability challenges. Finally, the current work does not integrate advanced security mechanisms such as blockchain-based audit trails or artificial intelligence-based anomaly detection. Incorporating such techniques in future work could improve traceability, intrusion detection, and resilience against sophisticated cyberattacks.

Privacy and Cybersecurity Considerations

The proposed framework addresses core cybersecurity principles,⁵⁰ including confidentiality,⁵³ integrity,⁵⁴ availability,⁵⁵ and controlled authorization,^{56–58} within THR management.⁵⁹ Confidentiality is enhanced through dual OTP-based verification, which restricts record access to sessions explicitly approved by both the patient and the treating physician. Integrity is supported by authenticated access control mechanisms that prevent unauthorized modification or retrieval of THRs. Availability is maintained through the lightweight architectural design, which avoids computationally intensive processes and ensures timely access for legitimate users. Furthermore, the transparency-driven dual-consent mechanism strengthens privacy protection by ensuring that patients and physicians are aware of external record access requests. Together, these measures contribute to a secure and privacy-aware THR access environment.

Conclusion

This article proposes a THR-maintenance framework that achieves transparency and security in THR access through a OTP mechanism. The THR manager is responsible for collecting and coordinating processes for maintaining health records, including user registration, login, OTP generation, and OTP verification. The proposed work is implemented using HTML-based web page development, and each stage of the web workflow was verified to support secure data access and transmission. The proposed framework enables transparent access to THRs, ensuring that both patients and physicians know when and how health records are accessed, including usage for research and disease analysis. This approach supports improved awareness, follow-up queries, and response mechanisms while maintaining controlled access to sensitive medical information. Performance evaluation indicates that the OTP delivery time is 15 ms, the API response time is 25 ms, and the THR load time is 15 ms. The overall authentication success rate achieved is 97%. In future work, this framework can be extended to support broader, global access to THRs, as well as enhanced scalability, auditability, and interoperability across healthcare platforms.

Funding

This research received no internal or external funding.

Financial and Non-Financial Relationships and Activities

Not applicable.

Data Availability Statement (DAS), Data Sharing, Reproducibility, And Data Repositories

Not applicable.

Application of AI-Generated Text or Related Technology

The authors confirm that AI tools were used only for language editing/grammar assistance, if applicable. AI tools were not used for data analysis, interpretation, or generation of scientific conclusions. No AI-generated images or figures were used in this manuscript. If used, they have been clearly disclosed and comply with the journal's guidelines.

Contributions

Not applicable.

Acknowledgments (Optional)

Not applicable.

References

- Ganesan B, Tong RKY. Chapter 1—Historical overview and the evolution of digital health. In: Tong RKY, Ganesan B, editors. *Digital technology in public health and rehabilitation care*. Academic Press; 2025. p. 3–18. ISBN 9780443222702.
- Vesselkov A, Hämmäinen H, Töyli J. Technology and value network evolution in telehealth. *Technol Forecast Soc Change*. 2018;134:207–22. <https://doi.org/10.1016/j.techfore.2018.06.011>
- Horsch A, Balbach T. Telemedical information systems. *IEEE Trans Inf Technol Biomed*. 1999;3(3):166–75. <https://doi.org/10.1109/4233.788578>
- Holmgren AJ, Thombley R, Sinsky CA, Adler-Milstein J. Changes in physician electronic health record use with the expansion of telemedicine. *JAMA Intern Med*. 2023;183(12):1357–65. <https://doi.org/10.1001/jamainternmed.2023.5738>
- Chumbler NR, Haggstrom D, Saleem JJ. Implementation of health information technology in Veterans Health Administration to support transformational change: Telehealth and personal health records. *Med Care*. 2011;49(Suppl):S36–42. <https://doi.org/10.1097/MLR.0b013e3181d558f9>
- Ambinder EP. Electronic health records. *J Oncol Pract*. 2005;1(2):57–63. <https://doi.org/10.1200/JOP.2005.1.2.57>
- Jacob PD. Management of patient healthcare information: Healthcare-related information flow, access, and availability. In: Gogia S, editor. *Fundamentals of telemedicine and telehealth*. Academic Press; 2020. p. 35–57.
- Kumar MS, Ganesh D. Improving telemedicine through IoT and cloud computing: Opportunities and challenges. *Adv Eng Intell Syst*. 2024;3(3):123–35. <https://doi.org/10.22034/aeis.2024.474171.1217>
- AlOsail D, Amino N, Mohammad N. Security issues and solutions in e-health and telemedicine. In: Pandian A, Fernando X, Islam SMS, editors. *Computer networks, big data and IoT*. LNDECT, vol 66. Springer; 2021.
- Ge S, Song Y, Hu J, Tang X, Li J, Dune L. The development and impact of adopting electronic health records in the United States. *Health Care Sci*. 2022;1(3):186–92. <https://doi.org/10.1002/hcs2.21>
- Costa RT, Adib K, Salama N, Davia S, Millana AM, Traver V, et al. Electronic health records and data exchange in the WHO European region. *Int J Med Inform*. 2025;194:105687. <https://doi.org/10.1016/j.ijmedinf.2024.105687>
- Ondogan AG, Sargin M, Canoz K. Use of electronic medical records in the digital healthcare system. *Inform Med Unlocked*. 2023;42:101373. <https://doi.org/10.1016/j.imu.2023.101373>
- Sivan R, Zukarnain ZA. Security and privacy in cloud-based e-health systems. *Symmetry*. 2021;13(5):742. <https://doi.org/10.3390/sym13050742>
- Oh SR, Seo YD, Lee E, Kim YG. A comprehensive survey on security and privacy for electronic health data. *Int J Environ Res Public Health*. 2021;18(18):9668. <https://doi.org/10.3390/ijerph18189668>
- Harris Y, Goldwater JC. Lack of evidence for telehealth fraud. *J Telemed Telecare*. 2023;31(2):301–5. <https://doi.org/10.1177/1357633X231177739>
- Kadakia KT, Howell MD, DeSalvo KB. Modernizing public health data systems. *JAMA*. 2021;326(5):385–6. <https://doi.org/10.1001/jama.2021.12000>
- Szalados JE. Medical records and confidentiality. In: *The medical-legal aspects of acute care medicine*. Springer; 2021.
- Subramanian H, Sengupta A, Xu Y. Patient health record protection beyond HIPAA. *J Med Internet Res*. 2024;26:e59674. <https://doi.org/10.2196/59674>
- Semantha FH, Azam S, Shanmugam B, Yeo KC, Beeravolu AR. A conceptual framework to ensure privacy in patient record management systems. *IEEE Access*. 2021;9:165667–89. <https://doi.org/10.1109/ACCESS.2021.3134873>
- Lalem F, Laouid A, Kara M, Al-Khalidi M, Eleyan A. A novel digital signature scheme for advanced asymmetric encryption. *Appl Sci*. 2023;13(8):5172. <https://doi.org/10.3390/app13085172>
- Hagui I, Msolli A, Ben Henda N, et al. A blockchain-based security system with light cryptography. *Multimed Tools Appl*. 2024;83:52451–80. <https://doi.org/10.1007/s11042-023-17643-5>
- Zeng D, Badshah A, Tu S, Waqas M, Han Z. A security-enhanced ultra-lightweight and anonymous user authentication protocol for telehealthcare information systems. *IEEE Trans Mobile Comput*. 2025;24(5):4529–42. <https://doi.org/10.1109/TMC.2025.3526519>
- Dahl-Popolizio S, Carpenter H, Coronado M, Popolizio NJ, Swanson C. Telehealth for occupational therapy during COVID-19. *Int J Telerehabil*. 2020;12(2):77–92. <https://doi.org/10.5195/ijt.2020.6328>
- Chattopadhyay A, Ho T, Beyene N. A W3H2 analysis of security and privacy issues in telemedicine. In: *Proc ACMSE '23*. ACM; 2023. p. 47–55. <https://doi.org/10.1145/3564746.3587109>
- AlAmr MI. Building patient trust through enhanced data security: A Saudi hospital case study. *Galore Int J Appl Sci Humanit*. 2024;8(4):25–33. <https://doi.org/10.52403/gijash.20240405>
- Vidanagamachchi S, Mallikarachchi S. Exploring privacy and security concerns in Sri Lankan telemedicine systems. *Sri Lankan J Appl Sci*. 2024;3(1):15–22.
- Insani WN, Zakiyah N, Puspitasari IM, et al. Digital health technology interventions for medication safety. *J Med Internet Res*. 2025;27:e65546. <https://doi.org/10.2196/65546>
- Rathee T, Tomer M, Chadha IK. Cloud computing applications in digital health. In: *Explainable IoT applications*. Springer; 2025. https://doi.org/10.1007/978-3-031-74885-1_5
- Manasa R, Jayanthiladevi A. CyVHealth: Intelligent cybersecurity architecture for virtual medical consultation. *Cybersecur Appl*. 2025;3:100112. <https://doi.org/10.1016/j.csa.2025.100112>
- Narayanasamy D. Transforming healthcare with secure cloud infrastructure. *Int J Sci Res Comput Sci Eng Inf Technol*. 2025;11:633–44. <https://doi.org/10.32628/CSEIT25111271>
- Patra D, Rajagopalan N. Integration of emerging technologies in cybersecurity for healthcare. *Comput Secur*. 2026;161:104763. <https://doi.org/10.1016/j.cose.2025.104763>
- Mahto D, Yadav D. Cloud-based secure telemedicine information system using crypto-biometric techniques. *EAI Endorsed Trans Pervasive Health Technol*. 2020. <https://doi.org/10.4108/eai.13-7-2018.163837>
- Suleski T, Ahmed M, Yang W, Wang E. Review of multi-factor authentication in IoHT. *Digit Health*. 2023;9. <https://doi.org/10.1177/20552076231177144>
- Zhang W, Hasan MK, Jailani NB, et al. Lightweight security model for telehealth confidentiality. *Comput Hum Behav*. 2024;153:108134. <https://doi.org/10.1016/j.chb.2024.108134>
- Ahmad RW, Salah K, Jayaraman R, et al. Role of blockchain in telehealth and telemedicine. *Int J Med Inform*. 2021;148:104399. <https://doi.org/10.1016/j.ijmedinf.2021.104399>
- Shrimali B, Surati S, Trivedi H. MediBlock: Blockchain-based secure healthcare architecture. In: *Proc InCACCT 2023*. IEEE; 2023. <https://doi.org/10.1109/InCACCT57535.2023.10141848>
- Kumar M, Raj H, Chaurasia N, Gill SS. Blockchain-inspired secure data exchange for healthcare 4.0. *IoT Cyber-Phys Syst*. 2023;3:309–22. <https://doi.org/10.1016/j.iotcps.2023.05.006>
- Odeh A, Abdelfattah E, Salameh W. Privacy-preserving data sharing in telehealth services. *Appl Sci*. 2024;14(23):10808. <https://doi.org/10.3390/app142310808>
- Lone SA, Mir AH. Novel OTP-based tripartite authentication scheme. *Int J Pervasive Comput Commun*. 2022;18(4):437–59. <https://doi.org/10.1108/IJPPCC-04-2021-0097>
- Akilan SS, Sekar JR. OTP-Q encryption and Diffie–Hellman authentication for e-healthcare data. *Technol Health Care*. 2023;31(6):2073–90. <https://doi.org/10.3233/THC-220588>
- Harshini BV, Ulagarchana U, Mounika P, Shamala LM. OTP verification and zero trust security for medical records. In: *Proc ICSTSN 2024*. IEEE; 2024. <https://doi.org/10.1109/ICSTSN61422.2024.10671108>
- Khan A, Khan SS, Shirazi ZY, et al. Hybrid mobile and web-based health record management system. In: *Proc ICAIQSA 2024*. IEEE; 2024. <https://doi.org/10.1109/ICAQSA64000.2024.10882381>

43. Dahal S. TelecarePLUS: An extensive telemedicine platform. Master's Thesis, Concordia University of Edmonton; 2023.
44. Ghanbari P. TelecarePLUS: Bridging the gap between providers and patients. Master's Thesis, Concordia University of Edmonton; 2023.
45. Shaibu IA, Caroline OA, Nathaniel S. Development of e-health portal with smart authentication. *J Eng Eng Technol*. 2024;18(1):20–33.
46. Zulkifl Z, et al. FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs. *IEEE Access*. 2022;10:15644–56. <https://doi.org/10.1109/ACCESS.2022.3149046>
47. Hegde G, Gupta S, Prabhu GM, Bhandary SV. EyeEncrypt: Secure retinal image segmentation. In: *ATIS 2022. CCIS, vol 1804*. Springer; 2023. https://doi.org/10.1007/978-981-99-2264-2_9
48. Khalid F, Abbas S, Sadeq A, Aslam B. Is information sharing during online medical consultations a patient's concern? An extended theoretical model. *Hum Behav Emerg Technol*. 2025(1):7342994. <https://doi.org/10.1155/hbe2/7342994>
49. Es-sabry M, El Akkad N, Merras M, Saaidi A, Satori K. New color image encryption algorithm. In: *Embedded systems and artificial intelligence*. Springer; 2020. https://doi.org/10.1007/978-981-15-0947-6_55
50. Alghamdi T, Gebali F, Salem F. Multifactor authentication for smart emergency medical response. *Int J Telemed Appl*. 2022. <https://doi.org/10.1155/2022/5394942>
51. Patel I, Jain S, Vishwajeet JK, Aggarwal V, Mehra P. Securing electronic healthcare records in web applications. *Int J Eng Adv Technol*. 2021;10(5). <https://doi.org/10.35940/ijeat.E2781.0610521>
52. Gupta S, Sharma HK, Kapoor M. Smart healthcare and telemedicine systems. In: *Blockchain for secure healthcare using IoMT*. Springer; 2023. https://doi.org/10.1007/978-3-031-18896-1_1
53. Sharma HK, Choudhury T, Mor A. Methodologies for improving telehealth quality and safety. In: *Telemedicine: The computer transformation of healthcare*. Springer; 2022. https://doi.org/10.1007/978-3-030-99457-0_14
54. Talal AH, Sofikitou EM, Jaanimägi U, et al. Patient-centered telemedicine framework. *J Biomed Inform*. 2020;112:103622. <https://doi.org/10.1016/j.jbi.2020.103622>
55. Deris MSM, Mohamed MA, Mohamed RR, et al. Challenges in access to health facilities for rural citizens. *Int J Eng Trends Technol*. 2021;69(8):36–40. <https://doi.org/10.14445/22315381/IJETT-V69I8P205>
56. Rajput AR, Masood I, Tabassam A, et al. Data privacy and security in mHealth applications. *Soft Comput*. 2023;27:18165–80. <https://doi.org/10.1007/s00500-023-09265-8>
57. Aggrey R, Adjei BA, Afoduo KO, Dsane NAK. Securing telehealth platforms. *Int J Multidiscip Res*. 2024;6(6).
58. Perez K, Wisniewski D, Ari A, et al. AI and telemedicine in rural communities. *Healthcare*. 2025;13(3):324. <https://doi.org/10.3390/healthcare13030324>
59. Uchechukwu BN, Ohinameuwa A. Enhanced health record information management system using mobile framework. *J Sci Technol*. 2025;30(3). <https://doi.org/10.20428/jst.v30i3.2750>

Copyright Ownership: This is an open-access article distributed in accordance with the Creative Commons Attribution Non-Commercial (CC BY-NC 4.0) license, which permits others to distribute, adapt, enhance this work non-commercially, and license their derivative works on different terms, provided the original work is properly cited and the use is non-commercial. See <http://creativecommons.org/licenses/by-nc/4.0>. The authors of this article own the copyright.