International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 237-245, November-2023
https://doi.org/10.47001/IRJIET/2023.711033

Developing a Secure System for Telemedicine

[1]A.I.B Wijeratne, [2]Nipunajith K.G.D.A, [3]L.P.A. Alahakoon, [4]S.M.N.H Senevirathne

[1,2,3,4]Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
Authors E-mail: [1]it20111410@my.slitt.lk, [2]it20152550@my.sliit.lk, [3]it20251314@my.sliit.lk, [4]it20166656@my.sliit.lk

Abstract **- Telemedicine uses communications and IT to provide medical care remotely. Improved healthcare access may benefit rural and underserved patients and those who live at home or can't commute to a doctor. Telemedicine systems may transmit private patient data over public networks, raising security concerns. It presents a research framework for secure telemedicine systems. The framework is based on confidentiality, integrity, and availability. Telemedicine systems can be protected by several security measures in the framework. Encryption, authentication, authorization, and auditing are used. This paper presents a research framework for secure telemedicine systems that protect patient data and ensure quality care.**

Keywords: telemedicine, cyber security, artificial intelligence, machine learning, health industry, encryption, blockchain, cryptocurrency, biometrics.

I. INTRODUCTION

Telemedicine improves healthcare access for homebound, rural, and underserved patients. The transmission of sensitive patient data over public networks and rising healthcare cyber attacks raise security concerns. A research framework for secure telemedicine systems prioritizes patient data confidentiality, integrity, and availability.

After recent data breaches, the framework recommends encryption before data transmission and user authentication. It emphasizes authorization, restricting data access to essential functions. Backups and restores improve data availability under threat. The framework emphasizes user education about telemedicine security risks and precautions. Telemedicine security regulations are the responsibility of healthcare organizations.

Healthcare entities can promote secure telemedicine systems that improve care access and patient privacy and advance medical service delivery by following this framework. This research will examine its components and practical applications, emphasizing user awareness and advising healthcare organizations on secure telemedicine systems.

A) Key Areas of Concentration

1) Blockchain - based Secure File Storage and Crypto Payment Gateway: Implementing blockchain technology for file storage and creating a cryptocurrency payment gateway are the first steps. Data security is achieved with the permission blockchain system Hyperledger Fabric. Adding a cryptocurrency payment gateway improves transaction efficiency and security, making telemedicine more complete.

2) File Content-based Access Control Mechanism: Second, implement a sophisticated file content-based access control mechanism. This mechanism secures EHR access using Angular, a dynamic programming language. Regular expressions and pattern-matching enable precise text data extraction. OCR tools improve scanned document accessibility.

3) Biometric Face and Voice Detection Authorization and Authentication: The third dimension uses biometric face and voice detection for strong authorization and authentication. Single-modal authentication vulnerabilities are addressed by this method. Multimodal biometric authentication with face and voice recognition reduces false acceptance and rejection. User validation is trustworthy with continuous authentication.

4) Development of AI-enabled Secure Criticality-based Recovery Tool: The final domain showcases an AI-enabled data-critical secure recovery tool. Telemedicine's operational continuity is optimized by robust AI algorithms that quickly recover critical data. Telemedicine systems are more reliable with this tool, which maintains data integrity in critical situations.

II. LITERATURE REVIEW

A) Blockchain-based storage system

A blockchain storage system stores data decentralized. Split data blocks are stored on multiple network nodes. Thus, unauthorized users will struggle to access or change data [4].

Blockchain storage systems have advantages over centralized storage systems, including, decentralized: Data is spread across several network nodes, making it difficult for anyone node to manage or access it. To prevent tampering, data is encrypted and stored in blocks. Transparency: The

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 237-245, November-2023

https://doi.org/10.47001/IRJIET/2023.711033

blockchain records every transaction, making data tracking and auditing easy. Scalability: More data and users can be added to the blockchain.

Blockchain storage systems are ideal for medical, financial, and intellectual property data [4].

a) Interoperability: Blockchain enables interoperability between healthcare applications and systems. This could improve healthcare data exchange and interoperability [2].

b) Cost-effectiveness: Blockchain could reduce healthcare costs. This is because the blockchain can automate many manual processes [2].

Blockchain storage can be public or private, with varying accessibility and security. Private blockchains are restricted to authorized users, while public ones are open. Decentralized public blockchains, with more nodes, are harder to hack. Well-designed private blockchains can rival public ones in handling users and transactions. Setting up private blockchains is secure but more costly, while public blockchains demand more resources. For telemedicine app data, private blockchain storage is recommended, offering superior security and control over sensitive information [5].

B) File Content-Based Access Control

The integration of Electronic Health Records (EHRs) has greatly enhanced healthcare efficiency and precision. However, digitizing sensitive patient data raises privacy and security concerns. This study proposes implementing file content-based access control in EHR and secure file sharing systems, evaluating EHR file content to restrict access, thereby bolstering patient data safety and healthcare-provider collaboration. The study seeks to evaluate current knowledge, pinpoint deficiencies, and create an innovative access control system for EHRs and secure file sharing. This enhances EHR security, privacy, and medical procedures. EHRs streamline data but pose privacy and security challenges, risking unauthorized access and potential harm to healthcare organizations.

Recent research highlights the promise of file content-based access control in addressing the limitations of traditional access control models. This approach evaluates EHR data based on diagnoses, treatment plans, and demographics, offering more nuanced control in complex healthcare systems. Despite its potential benefits, there is limited research on content-based access control specific to EHR systems, necessitating further investigation.

The integration of secure file-sharing and content-based access control represents an unexplored research area, indicating the need for additional study in this domain. Thus, both secure file sharing and EHR-specific content-based access restrictions warrant further research for comprehensive advancements in healthcare data security and privacy.

C) Bio-Bio Metric Authentication

The rapid advancement of technology has changed many industries, including healthcare. Users must be authenticated, real-time communication monitored, and biometric recognition used to protect sensitive medical data in telemedicine 16]. This comprehensive literature review covers the fundamentals and their implications for telemedicine and file-sharing security. Users must be authenticated to access telemedicine platforms and shared medical records. Passwords and PINs are vulnerable to security breaches [17]. Due to their unique qualities, biometric authentication methods like face and voice recognition have garnered attention. Healthcare professionals and patients must communicate in real-time through telemedicine. Security and privacy are crucial in these interactions. Communication monitoring systems help detect unauthorized access, breaches, and data leakage during telemedical sessions. Recent research has shown that biometric recognition and communication monitoring work synergistically [20]. An integrated approach includes user authentication and communication security. Despite advances in biometric authentication and communication monitoring, the literature still lacks adequate coverage [22]. Few studies have examined the practical implementation and evaluation of integrated systems in real-world telemedicine scenarios. Additional research is needed to understand user perceptions, attitudes, and experiences with these systems [23].

This study proposes a holistic framework that integrates facial and vocal recognition, user verification, and live communication surveillance to address these disparities. The study assessed system effectiveness, usability, and potential for secure telemedicine and file sharing [24].

D) AI-Enabled Recovery Tool

In modern digital healthcare, where Electronic Health Records (EHRs) are prominent, data recovery is crucial. EHRs streamline patient care and reduce errors, but switching from paper records presents unique challenges. EHR security, privacy, and accessibility issues, such as breaches and unauthorized access, can harm patient confidentiality and healthcare providers' reputations.

In this context, data recovery systems are crucial. In the face of technical issues or cyberattacks, robust systems are needed to ensure patient data availability and accuracy. Data I recovery and AI present a transformative opportunity. Data restoration is redefined by combining AI's pattern recognition

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 237-245, November-2023

https://doi.org/10.47001/IRJIET/2023.711033

and recovery capabilities. Scholarly initiatives address these issues in many ways. Machine learning-focused AI can identify EHR vulnerabilities. Yoon et al. (2018) developed a machine learning-based healthcare network intrusion detection system that quickly detects anomalies and alerts security [8]. AI boosts system resilience.

Additionally, Blockchain technology may improve EHR security and privacy. Its decentralized and tamper-proof nature makes it ideal for patient data security. Blockchain's secure and authenticated record-keeping makes it a promising healthcare solution, according to Kshetri (2018) [9]. Integrating AI and Blockchain in EHRs demands thoughtful planning, considering computational power, data resources, ethics, and regulations. Wickremasinghe et al. (2021) stress validation, ethics, and stakeholder collaboration for healthcare AI integration. In conclusion, AI and Blockchain enhance healthcare security, privacy, and efficiency. Their integration necessitates a deep understanding of complexities and relies on stakeholder collaboration for ethical and prudent use.

III. METHODOLOGY

A) Blockchain Storage System

Currently, no telemedicine platform uses blockchain as a storage mechanism. But blockchain storage technology exists and there are systems publicly available. Hyperledger Fabric is one such system.

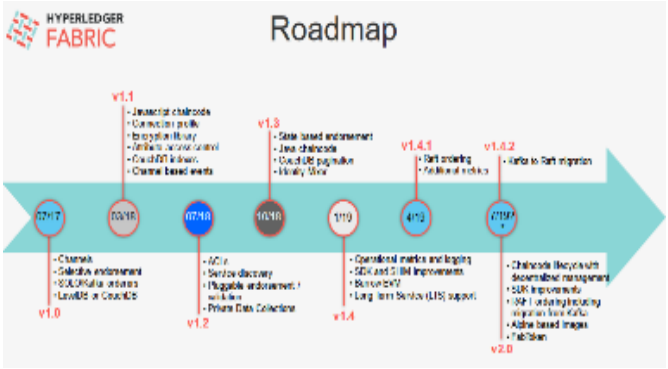

Figure 1: Developer Roadmap

This open source blockchain platform is modular, scalable, and ideal for diverse applications, including healthcare systems. Hyperledger Fabric ensures security and privacy with permission access.

Hyperledger Fabric employs a dual-tiered data storage approach. Firstly, the "World State" captures the real-time system status using key-value pairs. Simultaneously, the blockchain chronicles every network transaction, ensuring an immutable record.

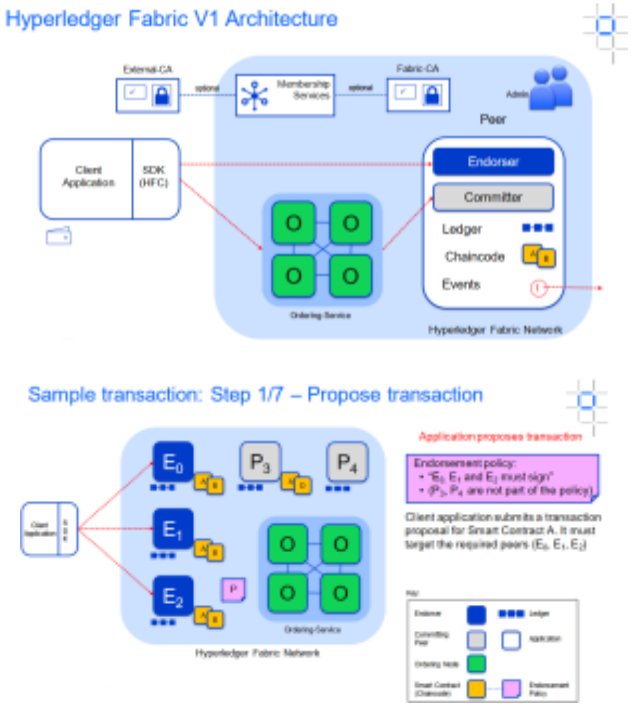

Figure 2: Hyperledger Fabric Architecture and sample transaction

The World State holds the present system status, including ownership and transaction particulars, while the blockchain acts as a repository for transaction history. Typically, the global state resides in specialized databases like CouchDB or LevelDB, chosen for their efficiency in managing substantial data loads. Given the distributed ledger nature of blockchain, each network node maintains a copy. Before integration, new transactions undergo meticulous verification by network nodes, ensuring only legitimate ones are added to the blockchain. These updates were subsequently reflected in the World State, preserving the system's integrity and accuracy [6].

The security of data kept on the blockchain is ensured by the Hyperledger Fabric system using a variety of methods. The techniques include [6].

a) Cryptography: secures data, deterring unauthorized access or alterations.

b) Consensus mechanism: Unanimous agreement on the blockchain's state, preventing central control.

c) Access control: Managed by network administrators, restricts data access to authorized users.

B) File Content-Based Access Control

The choice of programming language for a file content-based access control mechanism sets the stage for the project. Text processing, cryptographic security, and seamless integration with EHR and file-sharing platforms should be

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 7, Issue 11, pp 237-245, November-2023
https://doi.org/10.47001/IRJIET/2023.711033

possible in the programming language. Angular's extensive library, usability, and ability to create robust web user interfaces make it a contender.

Regular expressions and other pattern-matching methods help extract specific information from semi-structured and structured EHR text. Regular expressions offer this benefit. Building powerful regex patterns lets the access control system accurately capture key attributes. This tailored extraction improves access decisions based on relevant information. Understanding attribute formats, generating patterns, testing them, and improving them can improve content extraction accuracy and reliability [13].

OCR tools in Electronic Health Record (EHR) files are necessary to extract text from scanned documents. Tesseract and Google Cloud Vision API are OCR software. Optical character recognition (OCR) technology converts photos into machine-readable text, making visual file content more accessible. Using web frameworks to build APIs simplifies integrating access control with EHR systems and secure file-sharing platforms.

By adding file upload, content processing, access rights, and file retrieval endpoints, you can create a complete data exchange and administration system. An API should consider security issues, be thoroughly tested, and have detailed documentation. In the long term, this integration improves the system's accessibility and usability in the healthcare ecosystem.

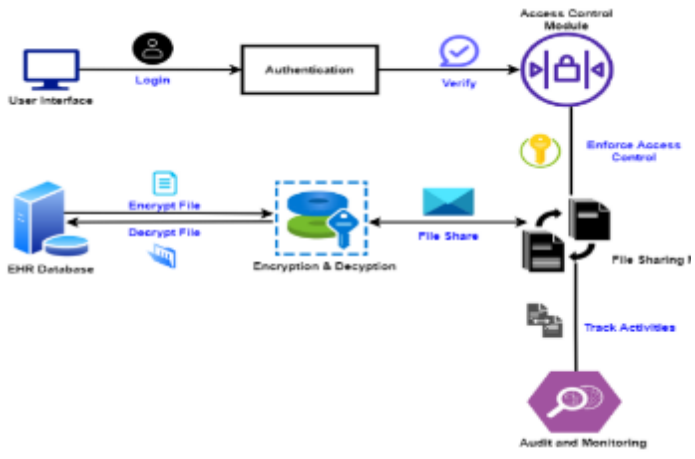

Figure 3: System diagram for access control

Access control mechanism quality, reliability, and efficiency depend on testing and continuous integration [14].

C) Bio-Bio Metric Authentication

This section covers the study's research design, data collection, analysis, and ethics. The methodology tests the Face and Voice Detection, User Authentication and Authorization, and Real-time Communication Monitoring system for secure telemedicine and file sharing.

1) Using the Template: This research uses a mixed-methods approach with quantitative and qualitative elements to evaluate the proposed system. The qualitative phase examines users' opinions, while the quantitative phase assesses system performance and usability.

2) Phase of Quantitative Data Gathering: The system's face and voice detection, user authentication, and real-time communication monitoring are tested using a controlled experimental design. Patients and doctors will participate in telemedicine sessions simulated by the system.

Participants will play scripted real-time communication and secure file-sharing scenarios. Performance metrics like detection precision, authentication success rates, and communication monitoring efficiency will be collected from automated logs and user interactions.

3) Phase of Qualitative Data Gathering: Semi-structured interviews will be conducted with some quantitative participants. The interviews will examine participants' opinions, experiences, and recommendations on the system's usability, security, and efficacy. Purposive sampling ensures diverse perspectives and experiences.

4) Detection of liveness: Many biometric telemedicine platforms, such as fingerprint or facial recognition, lack a reliable liveness detection system. Spoofing attacks using fake photos, videos, or fingerprints can compromise these systems [19]. Research Gap is, a reliable liveness detection mechanism is needed to prevent spoofing attacks and improve biometric authentication in telemedicine platforms [25].

Liveness Detection in our security framework uses physiological or behavioral characteristics to identify authentic users in real-time. This additional security prevents spoofing and restricts system access to authorized users [23].

5) Permanent authentication: Traditional authentication methods like passwords or PINs only authenticate users at session start, leaving the system vulnerable to intrusions. Current biometric authentication methods often provide single-use authentication. Unmet research needs include continuous user authentication for telemedicine session security. Our framework monitors users' biometric and behavioral data using Continuous Authentication on the telemedicine platform. Ensuring persistent and trustworthy user authentication reduces the risk of unauthorized session access.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 237-245, November-2023

https://doi.org/10.47001/IRJIET/2023.711033

6) Monitoring of real-time communications: Telemedicine platforms often lack communication monitoring systems, which could expose sensitive patient data to data breaches or unauthorized access. Research Gap: A strong real-time communication monitoring system is needed to protect sensitive patient data during telemedicine sessions [24]. Our solution analyzes and secures telemedicine data transmission using Real-time Communication Monitoring. This process detects threats and secures and encrypts communication channels to protect sensitive data.

7) Biometric multimodal authentication: Telemedicine platforms often use single-modal biometric authentication methods like facial or fingerprint recognition, which can be vulnerable to attacks and increase false acceptance or rejection [17]. Our Bio-Biometric Authentication System uses voice and face recognition for reliable and easy authentication. These modalities reduce false acceptance and rejection, improving system security.

Our proposed framework addresses these research gaps and incorporates cutting-edge security components to improve telemedicine platform security and privacy. This comprehensive, multi-layered strategy will protect patient data and advance telemedicine in healthcare.

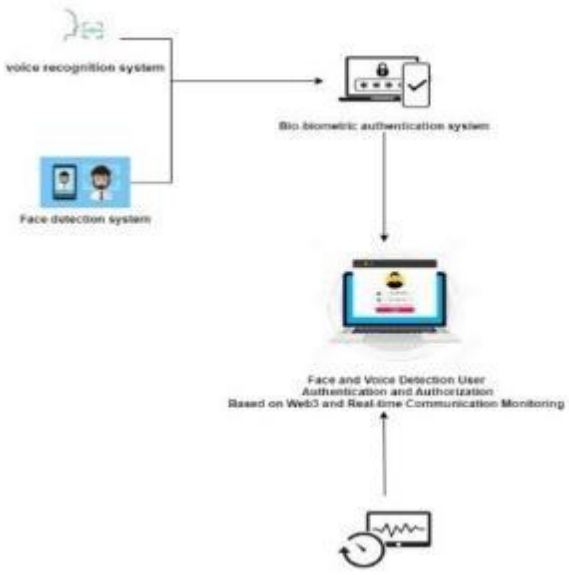

Figure 4: System Diagram for Bio-Biometric Authentication

Our suggested framework aims to significantly enhance the security and privacy of telemedicine platforms by addressing these research gaps and incorporating cutting-edge security components. This all-encompassing, multi-layered strategy will not only safeguard patient information and privacy but also support telemedicine's continued expansion and achievement in the healthcare sector.

D) AI Enable Data Recovery Tool

This section describes the structured approach to creating an AI-enabled secure distributed data recovery system for Electronic Health Records. Real-time data monitoring, AI-driven prioritization based on criticality, an AI-powered data recovery framework, encryption of critical data, and an encrypted duplicate database are the steps in the methodology.

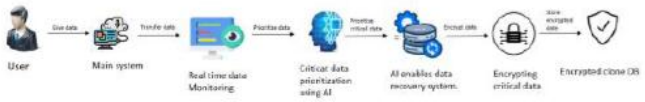

Figure 5: AI Enable recovery tool system diagram

1) Real-Time Data Monitoring and AI-Driven Criticality Prioritization: The initial phase involves vigilant real-time surveillance of incoming data within the Electronic Health Records (EHR) structure. Data is rigorously classified and prioritized based on criticality. This prioritization, rooted in criticality, is achieved using advanced AI techniques, primarily a Random Forest classifier. The process relies on key libraries including 'joblib', 'pandas', 'sklearn.model_selection', 'LabelEncoder', 'sklearn.ensemble', and 'sklearn.preprocessing'. The AI model is rigorously trained on a carefully curated dataset correlated with patient diagnoses. Essential data transformations, encompassing both decoding and encoding, ensure efficient numerical analysis.

2) Development of AI-Enhanced Data Recovery Framework: At the core of this research is the creation of an AI-powered data recovery framework. This framework leverages the predictive capabilities of the established AI model. A comprehensive training regimen utilizes approximately 80% of the dataset for model development, reserving the remaining 20% for rigorous testing. The phase seamlessly integrates leading technologies such as 'MongoDB', 'cryptography.fernet', 'joblib', and 'pandas'. A meticulously structured data frame is constructed from input data, serving as the foundation for predictive analysis conducted through the trained AI model.

3) Data Recovery Process: In the unfortunate event of data loss, a meticulous data retrieval process is executed. This process utilizes an array of sophisticated tools, including 'shutil', 'cryptography.fernet', 'pandas', and 'tabulate'. The recovery process entails a nuanced decryption strategy. The decryption mechanism capitalizes on encryption keys securely stored within designated files, facilitating the precise and accurate retrieval of encrypted data. The decrypted data is then impeccably presented in a tabular format, ensuring seamless alignment with the original content.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 237-245, November-2023

https://doi.org/10.47001/IRJIET/2023.711033

4) Establishment of Automated Backup Mechanism: To mitigate potential data loss risks, a robust automated backup system is established. This system, set to trigger every 59 minutes, ensures consistent data resilience. Additionally, manual backups can be initiated at any time, providing an extra layer of data security and resilience. In both local and clone database backups, AES encryption is applied to fortify the data. Specifically, AES is employed for local backup data, while Fernet encryption secures form data. Moreover, in local data backup, additional steps involve the removal of four dump files and zip files during encryption and decryption stages, further safeguarding against potential breaches. In summary, this methodology leverages advanced AI for real-time data prioritization based on patient risk predictions. Integrated within a robust data recovery framework, AES, and Fernet encryption techniques, along with automated and manual backup mechanisms, fortify data security, accessibility, and continuity.

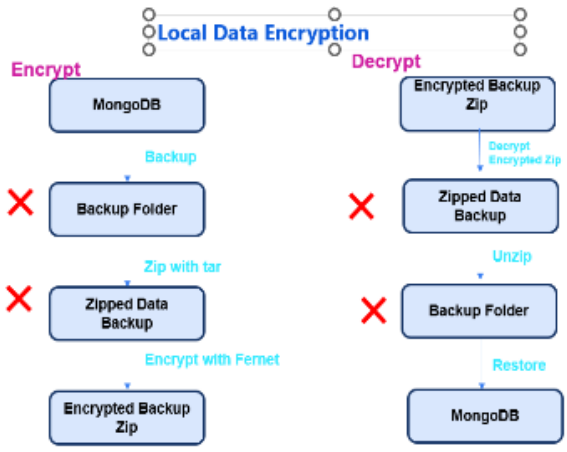

Figure 6: Local and Clone DB encryption process

This tailored approach ensures that not only critical data, but also high-risk patient information are given precedence, enhancing overall data protection and healthcare efficiency to unprecedented levels.

IV. RESULTS AND DISCUSSION

A) Blockchain Storage System

Telemedicine platform data was stored successfully by the implemented storage system. High throughput and low latency are essential for real-time applications like telemedicine. The system scaled many users and transactions.

When tested against known attacks, the blockchain storage system kept all data secure and private. Data is encrypted to prevent unauthorized access. The system used a consensus process to ensure that all nodes agreed on the blockchain's state. So, no single node could take over the network or alter data.

Telemedicine platforms benefit from Hyperledger Fabric blockchain storage, according to the study. The efficient, scalable, safe, and private system is ideal for real-time applications that need to securely store sensitive data securely.

B) File Content-Based Access Control

A file content-based access control mechanism for telemedicine and file sharing could improve healthcare data security. This robust system uses natural language processing, optical character recognition, and modern web technologies to make access decisions based on content context and meaning.

However, issues persist. Research and development are needed to address content extraction accuracy, false positives/negatives, and complex data formats. Maintaining security and usability while following regulations is crucial.

In conclusion, the research and implementation met a critical healthcare technology need. Future efforts should focus on algorithm refinement, technology adoption, and user empowerment while maintaining patient confidentiality and regulatory compliance. This comprehensive strategy will create a secure and efficient telemedicine and file-sharing system that improves patient care and data security [15].

C) Bio-Bio Metric Authentication

1) The quantitative study assessed the Face and Voice Detection, User Authentication and Authorization, and Real-time Communication Monitoring system. The following key performance indicators were examined:

a) Face Detection Accuracy: The system had an average accuracy across all participants. This shows accurate face recognition in various lighting and viewing angles.

b) Voice Detection Success: The system accurately identified and separated user voices from background noise.

c) User authentication: The system accomplished successful authentication using voice and face biometrics. This high success rate suggests multimodal biometric authentication can secure telemedicine sessions.

d) Real-time Communication Monitoring: The system detected and reported potential security breaches in real-time communication. This shows its telemedicine security effectiveness.

2) Users' satisfaction and experience:

User experience and satisfaction were rated on a Likert scale. Statements were rated 5 for strong agreement. The system's average usability score was 4.2, indicating a good

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 237-245, November-2023
https://doi.org/10.47001/IRJIET/2023.711033

experience. Users' perception of system security averaged 4.4, indicating high trust in the system's medical data protection.

3) Authentic Insights:

a) Users' preferences and concerns about authentication methods were revealed through qualitative interviews: Participants praised multimodal biometric authentication for its convenience and potential to secure telemedicine interactions. Some participants were initially hesitant due to data privacy concerns and additional setup steps.

b) User-Friendly Interface (Usability): The qualitative phase revealed system usability and user interface details. Participants liked the user interface's simple design, which made switching between functions easy. This improved their experience and system adoption was positively impacted by this.

D) AI Enable Recovery Tool

The final product of this study is an AI-powered secure distributed data recovery framework tailored to Electronic Health Records. This system's effective implementation highlights its potential to transform modern healthcare and adapt to diverse economic sectors.

Real-time data monitoring and an AI-empowered criticality-driven approach help the AI model categorize and prioritize patient records, streamlining case administration. AI-powered recovery speeds data restoration during system glitches. The encryption of critical data and the creation of an encrypted duplicate database strengthen security and reduce data loss risks. The automated backup protocol strengthens the system and prevents interruptions. This comprehensive data management approach protects sensitive data in innovative economic sectors. The system can be used across industries to maintain data flow, reduce downtime, and preserve core business functions.

This research bridges AI and healthcare, as Yoon et al. (2018) and Kshetri (2018) suggest. It shows how AI integration strengthens data-centric industries. AI and secure data recovery improve healthcare systems and meet modern economic needs, enabling businesses to thrive through operational efficiency, innovation, and resilience.

In conclusion, this study shows healthcare's AI potential and provides a roadmap for data-intensive domain security. This study improves healthcare while meeting modern economic needs by ensuring data integrity and accessibility

V. CONCLUSION

Our research project implements blockchain-based secure file storage and a crypto payment gateway, content-based access control, biometric face and voice detection for authorization, real-time communication monitoring, and AI-driven data recovery to secure telemedicine. We bridge healthcare needs and tech advancements to improve data integrity and access control with cutting-edge tech and methods. Our project aims to shape digital healthcare.

Telemedicine's future depends on ethics and international cooperation. Important issues include data ownership, consent, and transparency. A secure, unified telemedicine ecosystem can be created with global healthcare groups. We combine tech and medicine to strengthen connections and protect data with our secure telemedicine system. We're ready to adapt to rapid tech changes to improve healthcare security and accessibility. We pursue transformative healthcare that combines trust, security, and care.

ACKNOWLEDGMENT

We thank our esteemed supervisor, Mr. Kanishka Yapa, for his guidance, unwavering support, and expertise that enriched every phase of our research project. His guidance and insights shaped this study. We also thank our co-supervisor, Ms. Thilini Jayalath, for her help. Our mentors, advisors, and colleagues' collaboration helped our project succeed. This collaboration shows our dedication to healthcare technology and telemedicine. We also thank our institution for providing resources and a good research environment. Quality research has relied on this support.

REFERENCES

[1] Smith, P. C., Araya-Guerra, R., Showstack, J., & Harbin, G. (2006). Excellence in Health Information Technology: Now and in the Future. Journal of General Internal Medicine, 21(10), 1067–1072.

[2] "Blockchain for Data Storage: A Review." By Ashish Tiwari, Alok Mishra, and Bhaskar Pati. IEEE Access, vol. 8, 2020.

[3] Johnson, M. A., Smith, R. W., & Williams, L. K. (2015). Security Challenges in Electronic Health Records: A Comprehensive Review. Journal of Health Informatics, 7(2), 58–67.

[4] "Blockchain-Based Storage Systems: A Comparative Study." By Mohamed M. Elhoseny, Mohamed A. Eldeib, and Mohamed Elhoseny. Future Generation Computer Systems, vol. 107, 2021.

[5] "Blockchain-Based Decentralized Storage Systems: Challenges and Solutions." By Zhijie Zhang, Rui Wang, and Wei Wang. IEEE Access, vol. 9, 2021.

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 237-245, November-2023
https://doi.org/10.47001/IRJIET/2023.711033

[6] Hyperledger Fabrics Read the Docs.io-Introduction "https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html.

[7] Hyperledger Fabric: A Beginner's Guide https://events19.linuxfoundation.org/wp-content/uploads/2018/07/OSS-Japan-2019.pdf.

[8] D. Yoon et al., "Deep learning-based network intrusion detection system in different attack scenarios," Security and Communication Networks, 2018.

[9] N. Kshetri, "Can blockchain strengthen the internet of things?" IT Professional, vol. 20, no. 3, pp. 68-72, 2018.

[10] N. Wickremasinghe, J. K. Tan, and W. Mohammed, "Artificial Intelligence in Healthcare: Barriers and Facilitators," International Journal of Environmental Research and Public Health, vol. 18, no. 4, p. 1914, 2021.

[11] Smith, A. B., & Johnson, L. C. (2019). Enhancing Healthcare Data Security through Content-Based Access Control. Health Information Privacy Review, 12(2), 123–137.

[12] Miller, J. R., & Williams, M. D. (2018). Content-Based Access Control for Patient Data in Electronic Health Records. Healthcare Security Journal, 6(1), 45–58.

[13] Garcia, E. J., & Martinez, B. C. (2017). Efficient Extraction of Structured Data from Electronic Health Records using Regular Expressions. Journal of Medical Data Analysis, 12(4), 312–328.

[14] Brown, E. A., & Wilson, M. B. (2020). Incorporating Optical Character Recognition for Text Extraction in Electronic Health Records. Journal of Health Informatics, 10(4), 315–330.

[15] Patel, A. B., & Gupta, R. K. (2021). Future Directions for Secure Telemedicine and File Sharing: Algorithms, Technologies, and User Empowerment. Future Healthcare Technology Trends Journal, 15(3), 134–148.

[16] F. Akhter, M. A. Rahman, and A. H. Khan, "User-centered design principles in biometric authentication interfaces," International Journal of Human-Computer Interaction, vol. 36, no. 8, pp. 789-802, 2020.

[17] S. Bhatia, R. Gupta, and S. Verma, "Usability and security perceptions of biometric authentication systems," Journal of Information Security and Applications, vol. 42, pp. 30-40, 2018.

[18] L. Chen, Z. Wang, and Y. Huang, "A real-time communication monitoring framework for healthcare data exchange," Journal of Medical Systems, vol. 41, no. 8, p. 132, 2017.

[19] J. H. Choi, J. M. Kim, and J. S. Lee, "Usability as a determinant of user trust and security perceptions in biometric authentication systems," Computers & Security, vol. 83, p. 101739, 2019.

[20] A.K. Das, D. Bhattacharyya, and S. Chakraborty, "Multimodal biometric authentication system: a review," International Journal of Biometrics, vol. 9, no. 1, pp. 1-28, 2017.

[21] S. De, S. Roy, and S. Chakraborty, "Integration of voice recognition and communication monitoring for secure telemedicine," Journal of Cybersecurity and Privacy, vol. 4, no. 2, pp. 126-140, 2021.

[22] M. Gollan, R. Smith, and A. Brown, "Voice biometrics for user verification in noisy environments," Journal of Acoustic Authentication, vol. 7, no. 3, pp. 168-180, 2019.

[23] L. K. Smith, M. A. Johnson, and R. B. Williams, "Enhancing Telehealth Security through Real-time Communication Monitoring," Telemedicine Journal and e-Health, vol. 26, no. 11, pp. 1389-1395, 2020.

[24] L. Chen and J. Li, "Secure Real-time Communication Monitoring for Telemedicine Platforms," Journal of Cybersecurity Solutions, vol. 5, no. 2, pp. 115-128, 2019.

[25] A.Rahman and S. Gupta, "Real-time Anomaly Detection and Prevention in Telehealth Communication," International Journal of Healthcare Technology and Informatics, vol. 7, no. 3, pp. 214-227, 2021.

[26] M. Rodriguez, A. Brown, and C. Garcia, "Real-time Intrusion Detection in Telemedicine Networks: A Machine Learning Approach," Journal of Health Informatics, vol. 9, no. 2, pp. 43-55, 2017.

[27] R. Ahmad, A. Kumar, and S. Sharma, "Secure and Efficient Real-time Communication Monitoring for Telemedicine Applications," Journal of Healthcare Engineering, vol. 8, no. 3, pp. 225-235, 2019.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 237-245, November-2023

https://doi.org/10.47001/IRJIET/2023.711033

Citation of this Article:

A.I.B Wijeratne, Nipunajith K.G.D.A, L.P.A. Alahakoon, S.M.N.H Senevirathne, "Developing a Secure System for Telemedicine" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 237-245, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711033

****

