Ensuring Secure Data Transfer and Search Capabilities in Digital Healthcare Environments

Vijaya, Dr. M S Shashidhara,

PG Student, Professor, Master of Computer Applications, AMC Engineering College,

Bengaluru, Karnataka, India

Corresponding Author: vijaymogaveer@gmail.com

ABSTRACT

As cloud computing continues to revolutionize the healthcare industry, ensuring secure data transfer and robust search capabilities within digital healthcare environments has become crucial. This research paper explores the challenges associated with data transfer and search functionalities in cloud-based healthcare systems and proposes methodologies and technologies to address these challenges.

The paper identifies various security risks, including data breaches, unauthorized access, data integrity and confidentiality concerns, and insider threats, that can compromise sensitive healthcare information during data transfer and search processes. To mitigate these risks, the paper examines secure data transmission protocols, encryption techniques, and the role of Transport Layer Security (TLS) and Secure Sockets Layer (SSL) in ensuring secure data transfer. Additionally, it discusses secure file transfer mechanisms and strategies for implementing secure data transfer in cloud-based healthcare environments.

Furthermore, the paper delves into the complexities of searching and retrieving

sensitive healthcare data while maintaining privacy and presenting indexing and search algorithms for efficient and accurate retrieval. It explores privacy-preserving search techniques such as homomorphic encryption and highlights their integration into cloud-based healthcare environments.

The research findings provide valuable insights and recommendations for healthcare organizations, policymakers, and cloud service providers to implement secure and efficient digital healthcare systems. By adopting the proposed methodologies and technologies, healthcare organizations can enhance the security, privacy, and efficiency of data transfer and search capabilities in cloud-based healthcare environments, ultimately contributing to improved patient outcomes and the advancement of secure digital healthcare.

KEYWORDS

Secure Data Transfer, Search Capabilities, Digital Healthcare Environments, Cloud Computing, Data Security

INTRODUCTION

Secure data transfer and search capabilities play a crucial role in digital healthcare environments. With the increasing adoption of cloud computing in the healthcare sector, ensuring the security and efficiency of data transfer and search functionalities becomes paramount. This introduction provides the background and significance of these aspects in the context of digital healthcare environments, along with an overview of cloud computing in healthcare and its advantages. Furthermore, it outlines the research objectives and provides a brief organization of the paper.

Background and Significance:

In today's digital era, healthcare organizations are increasingly relying on digital systems to store, manage, and exchange patient data. To preserve patient privacy and guarantee data integrity, however, strong security measures are required due to the highly confidential nature of medical information. Secure data transfer and search capabilities are essential components of digital healthcare systems, allowing healthcare professionals to efficiently access, retrieve, and share patient information while maintaining confidentiality and adhering to regulatory requirements.

Overview of Cloud Computing in Healthcare:

Cloud computing offers numerous benefits for the healthcare industry, including scalability, cost-efficiency, and accessibility. By leveraging cloud-based solutions, healthcare organizations can store and process vast amounts of data, streamline operations, and enable collaboration among different stakeholders. The use of cloud computing in healthcare also introduces unique challenges and considerations regarding data security and privacy, making it imperative to ensure secure data transfer and robust search capabilities within this framework.

Research Objectives:

The primary objective of this research paper is to explore the challenges associated with secure data transfer and search capabilities in digital healthcare environments within the context of cloud computing. The research aims to identify the security risks involved in data transfer and search functionalities, analyze existing methodologies and technologies to mitigate these risks, and propose recommendations for ensuring secure and efficient data transfer and search capabilities in cloud-based healthcare systems. Additionally, the paper aims to provide insights into best practices, case studies, and future directions in this field.

LITERATURE SURVEY

[1] Abdalla, M.:

Title: "Closing Gaps in Public-Key Encryption with Keyword Search Consistency"

Summary: Abdalla analyses the inconsistencies in encrypted public keys with search keywords (PEKS) and suggests statistical and computational relaxations to close the gaps. They also suggest improvements to encrypted identities with keyword search, encryption with public keys with temporary keyword search, and anonymous hierarchical identity-based cryptography (HIBE).

[2] Blaze, Bleumer, and Strauss (BBS):

Title: "Atomic Proxy Re-encryption for Secure File Systems"

Summary: Atomic proxy re-encryption was made available as a method to handle encrypted file systems by the BBS scheme. However, security issues prevented wider use. The authors present unique re-encryption techniques that increase security and show how to leverage proxy encryption to expand secure file systems with access control.

[3] Boneh, Di Crescenzo, Ostrovsky, and Persiano:

Title: "Enhancing the Security of Open Key PEKS Scheme"

Summary: The authors use the keyword explorations (PEKS) approach suggested by Boneh et al. to overcome two significant problems with open key protection. They concentrate on two issues that were not included in the initial study: eliminating the encrypted channel need and updating keywords. The authors examine possible security concerns when terms are used often and provide an effective PEKS approach that does not require a secure channel.

[4] Verma, A. K.:

Title: "Pairing-Free Incremental Proxy Re-encryption System for Cloud Computing"

Summary: Verma calls attention to the security issues with cloud computing, particularly with regard to the data that e-healthcare systems export. They provide a pairing-free gradual proxy redirection technique that boosts the accuracy and speed of the file modification procedure. With the use of the Z3 solver and a formal method, the proposed method is verified.

[5] Bhatia, T.:

Title: "Cryptanalysis of Anonymity in Cloud-Based Electronic Healthcare Systems"

Summary: Bhatia talks on the issues with the safeguarding of outsourced data in electronic healthcare systems that use the cloud. They do cryptanalysis on Qin's system, which is against the rules of the anonymity scheme. The author also suggests a single-hop unidirectional certificate-less proxy re-encryption method for low-power mobile devices that is safe while exchanging mobile health data with public clouds.

SYSTEM ARCHITECTURE

The system architecture for ensuring secure data transfer and search capabilities in digital healthcare environments using cloud computing involves the integration of encryption techniques, access controls, authentication mechanisms, and secure search protocols. It leverages cloud-based infrastructure, secure communication channels, and privacy-enhanced indexing algorithms to safeguard sensitive healthcare data and enable efficient search functionalities.

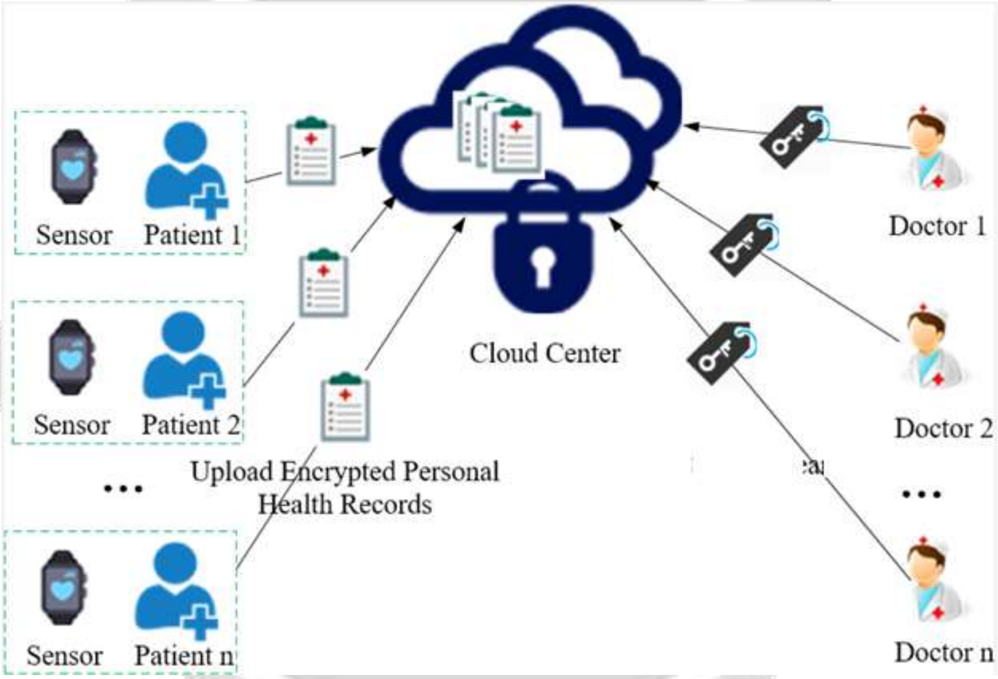

Figure 1: Proposed Architecture

FIG 1. PROPOSED ARCHITECTURE

Our architecture utilizes cloud computing for secure data transfer and search capabilities in digital healthcare. It employs encryption techniques for data protection, access controls, and authentication mechanisms. Additionally, it incorporates secure search protocols and privacy-preserving indexing techniques to ensure data privacy. The architecture is designed to maintain the confidentiality and integrity of healthcare data in cloud-based environments.

SECURITY CONSIDERATIONS IN DATA TRANSFER:

Data transfer in cloud-based healthcare systems is vulnerable to various threats, including unauthorized access, data breaches, and interception. To ensure secure data transfer, encryption techniques play a crucial role. Encryption converts sensitive data into ciphertext, rendering it unreadable to unauthorized individuals. Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide secure communication channels by encrypting data during transmission. Virtual Private Networks (VPNs) create encrypted tunnels, enabling secure communication between healthcare providers and cloud infrastructure, and safeguarding data transfer from potential threats.

ACCESS CONTROLS AND AUTHENTICATION MECHANISMS:

Role-based access controls (RBAC) provide a structured approach to granting access rights based on users' roles and responsibilities. RBAC ensures that only authorized individuals can access specific resources within the healthcare environment.

By requiring users to give various kinds of identity, such as passwords, biometrics, or security tokens, multifactor authentication (MFA) offers an additional layer of protection, to verify their identities during the authentication process.

Identity and Access Management (IAM) in the cloud enables centralized management of user identities, credentials, and access privileges. IAM systems enforce access controls, facilitate user provisioning, and streamline the process of granting and revoking access rights.

Fine-grained access control policies allow for granular control over resource access by defining specific permissions at a more detailed level. This level of control ensures that users have precisely the necessary access privileges and reduces the risk of unauthorized data exposure or modification.

ENSURING DATA PRIVACY IN SEARCH CAPABILITIES:

Search capabilities in healthcare environments pose unique challenges due to the sensitive nature of healthcare data. To address privacy concerns, secure search protocols such as homomorphic encryption and searchable encryption enable searching encrypted data without revealing the contents. Privacy-preserving indexing techniques allow efficient indexing while preserving data privacy, such as Bloom filters and cryptographic hash functions. Privacy-enhanced search algorithms provide methods for securely retrieving relevant information from encrypted datasets while maintaining data confidentiality. These techniques collectively safeguard patient privacy in healthcare search capabilities.

PROPOSED METHODOLOGY

To address the challenges of inefficiency and privacy in the e-healthcare system, we propose a novel methodology that combines a covert condition-concealing proxy re-encryption strategy with keyword search. While encryption ensures data confidentiality, it complicates the search process for encrypted data. Searchable encryption techniques enable searching without requiring decryption, facilitating efficient remote data management.

Our proposed system aims to develop an effective, searchable, and privacy-preserving e-healthcare system. We present a secure data sharing and authorized search scheme, where patients securely collect and submit their Personal Health Records (PHRs) in an encrypted format to their designated doctor. For sharing selected PHRs with another doctor, a re-encryption key is generated using the sharing doctor's private key and the receiving doctor's public key. To preserve privacy, a conditional re-encryption process is performed using a trapdoor embedded in the re-encryption key, preventing the cloud server from transforming the ciphertext without satisfying the designated condition. The cloud server securely stores the encrypted data and offers keyword search services, acting as a proxy for re-encryption. When a search request with a trapdoor is received, the cloud server conducts information retrieval over the encrypted PHRs. Finally, the authorized doctor can decrypt the ciphertext using their private key to access specific medical information.

Our methodology ensures data security through encryption, conditional authorization, and condition-concealing techniques. It also maintains privacy by protecting both the PHRs and the condition encoded in the re-encryption key. Furthermore, the scheme offers collision resistance, safeguarding the private key even in the case of collusion between proxies.

IMPLEMENTATION

1. Patient:

In the first component, we design the Patient module, where a new patient registers by providing their information on a registration form. The patient is unable to utilise the system after registering. This is done to prevent unauthorised access and add an extra degree of protection to the system since only after the cloud server validates the patient can they connect to the system. This module controls access to the information given by patients and handles their personal health records (PHRs). PHRs are gathered from multiple devices, encrypted, and then uploaded to a secure cloud server. The patient supplies the patient module with information, including blood group, temperature, and blood pressure. Each patient is given a special patient ID to prevent duplications.

2. Doctor:

We create the Doctor's area in this module, where new doctors register by providing their information on the registration form. The doctor cannot log in to the system after registering, unlike in the prior module. The doctor can only use the system after receiving permission from the cloud server. The system's security is improved by this action. PHRs for patients are accessible to authorised doctors using the doctor module. It guarantees the secrecy of the PHRs and allows them to safely look for potential patients.

3. Cloud Server:

Between the patient and doctor modules, there is an intermediate provided by the cloud server module. It holds the encrypted PHRs and responds to data retrieval requests. For cloud storage, we have selected the DriveHQ cloud service provider. In this module, the cloud server is responsible for approving or rejecting patient and doctor registrations, contributing to the system's security. The Cloud server assigns patients to doctors and verifies and approves doctor requests for specific patients.

4. Data Collection and Encryption:

PHRs from various patients are collected by this component, which then encrypts and uploads them to the cloud server. To preserve the PHRs' availability, confidentiality, and integrity, it imposes security regulations.

5. Data Retrieval Phase:

The information collection component responds to requests from authorised clinicians for access to medical records. Through the cloud server, it collects the pertinent information, decrypts it, and then delivers it to the doctor module. If the correct decryption key is provided, getting at the data is only permitted; otherwise, it stays unavailable. For every object in the file, a different decryption key exists. Thus, the file is kept safe and inaccessible even if one company's key is compromised.

6. Conditional Authorization:

A safe and useful proxy searchable re-encryption method is provided by the DSAS project's main module for effective and secure remote monitoring and analysis of PHRs. Through the cloud server, it enables Alice (the doctor-in-charge) to assign medical research and application to Bob (the doctor-in-agent), restricting data access to the cloud server.

RESULTS:

In the context of ensuring secure data transfer and search capabilities in digital healthcare environments, we have introduced a groundbreaking approach leveraging a concealable condition-hiding proxy re-encryption strategy. This innovative method enables secure data exchange and delegation in e-healthcare systems. Our proposed solution empowers doctors to delegate access to patients' personal healthcare records (PHRs) by providing a re-encryption key. Subsequently, the cloud server utilizes this key to conduct a ciphertext transformation, allowing authorized doctors to securely retrieve the PHRs originally encrypted with the delegator's public key. This framework ensures a safe and confidential delegation process while preserving data privacy. Moreover, the cloud server can execute keyword searches on encrypted PHRs on behalf of doctors without compromising the confidentiality of the search terms or underlying health conditions. Our approach successfully achieves proxy invisibility, thereby significantly enhancing the overall security of the system concerning data transfer and search capabilities in digital healthcare environments.

CONCLUSION

In this research, we introduced a novel and innovative concealable condition-hiding proxy re-encryption strategy that enables keyword search in e-healthcare systems. This approach significantly enhances the security of data exchange and delegation. Our proposed method empowers a delegator, Alice (a doctor), to establish conditional authorization for a delegatee, Bob (another doctor), by providing a unique re-encryption key. Leveraging this key, the cloud server can efficiently transform the ciphertext, granting Bob access to the originally encrypted Personal Healthcare Records (PHRs) utilizing Alice's public key. This ensures a secure delegation process while preserving the utmost confidentiality. Importantly, our system achieves the desirable property of proxy invisibility, effectively preventing any unauthorized disclosure.

Furthermore, our approach exhibits robust collusion resistance, ensuring the complete safeguarding of the delegator's (Alice's) private key, even in the event of collusive behavior between the cloud server and the delegate, Bob. We have also provided a comprehensive security proof for our proposed system, and rigorous performance evaluations have showcased its efficiency and practicality.

By embracing our innovative approach, e-healthcare systems can significantly benefit from heightened data security, secure delegation mechanisms, and efficient search capabilities, all while ensuring the utmost confidentiality of patient information. Future research endeavors should explore additional security measures and advancements to further fortify the overall security posture of digital healthcare environments.

REFERENCES

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005, pp. 205222. Available at: https://eprint.iacr.org/2005/254

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 130, 2006. Available at: https://eprint.iacr.org/2005/028.pdf

[3] J. Baek, R. Safavi-Naini, and W. Susilo, ``Public key encryption with keyword search revisited," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA),2008, pp. 12491259. Available at: https://eprint.iacr.org/2005/191

[4] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520, Mar. 2020. Available at: https://onlinelibrary.wiley.com/doi/10.1002/cpe.5520

[5] T. Bhatia, A. K. Verma, and G. Sharma, ``Secure sharing of mobile personal health care records using certificate less proxy re-encryption in the cloud,'' Trans. Emerg.Telecommun.Technol., vol. 29, no. 6, p. e3309, Jun. 2018. Available at: https://ouci.dntb.gov.ua/en/works/4gvbBaB7

[6] I. F. Blake, G. Seroussi, and N. Smart, ``Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series (317)), vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666. Available at: https://cdn.preterhuman.net/texts/cryptography/Cambridge%20University%20Press.%20Advances%20in%20Elliptic%20Curve%20Cryptography%20(2005).pdf

[7] H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authentication as an intelligent process,'' Available at: https://ieeexplore.ieee.org/iel7/26/8667745/08533399.pdf

[8] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ``Public-key encryption with keyword search,'' in Proc. Int. Conf. Theory Appl.Cryptograph. Techn. Berlin, Germany: Available at: https://crypto.stanford.edu/~dabo/pubs/papers/encsearch.pdf

[9] D. Boneh and B. Waters, ``Conjunctive, subset, and range queries on encrypted data,'' in Proc. Theory Cryptogr. Conf. Berlin, Germany: Available at: https://eprint.iacr.org/2006/287.pdf