OPEN ACCESS

Volume: 11

Special Issue: 1

Month: July

Year: 2023

E-ISSN: 2582-0397

P-ISSN: 2321-788X

Impact Factor: 3.025

Received: 04.5.2023

Accepted:22.6.2023

Published: 01.07.2023

Citation:
Deepa, KR, and K. Chandan. "DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System." *Shanlax International Journal of Arts, Science and Humanities*, vol. 11, no. S1, 2023, pp. 49–57.

DOI:
https://doi.org/10.34293/sijash.v11iS1-July.6315

DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System

Deepa K.R
Deparatment of Master of Computer Applications
Rajarajeswari College of Engineering

Chandan K
Deparatment of Master of Computer Applications
Rajarajeswari College of Engineering

Abstract

A rising number of people benefit from high-quality medical services in the e-healthcare system by exchanging encrypted personal healthcare records (PHRs) with doctors or medical research institutes. How-ever, one significant difficulty is that encrypted PHRs inhibit effective information search, resulting in a decrease in data utilisation. Another difficulty is that the medical treatment procedure necessitates the doctor being online at all times, which may be costly for all professionals (e.g., being absent under certain conditions). In this study, we propose a novel secure and practical proxy searchable re-encryption system that will enable medical care providers to conduct remote PHR monitoring and research in a safe and efficient manner. Through our DSAS scheme, (1) patients' medical information collected by the gadgets are protected by encryption before being put online in the cloud server, ensuring the security and confidentiality of PHRs; (2) only authorised doctors or academic institutions have having access to PHRs. Alice (doctor-in-charge) can delegate medical research and utilisation to Bob (doctor in agent) or a specific research institution via the cloud server, thereby minimising information exposure to the cloud. We formalise the security concept and demonstrate the scheme's security. Finally, performance evaluation demonstrates the effectiveness of our method. Proxy re-encryption, proxy invisibility, searchable encryption, mobile health care sensor networks.

Introduction

With the fast evolution of artificial intelligence and wearable devices and sensors, the e-healthcare sensor network has reached a degree of maturity for commercial acceptance and implementation. The use of an e-healthcare sensor network as a mobile platform greatly benefits patients in receiving high-quality and efficient medical treatment. As illustrated in Fig patients' devices capture a vast quantity of personal healthcare information via sensor devices, allowing clinicians to more efficiently diagnose and treat patients by using this data. This data also allows medical researchers and analysts to undertake analytics to acquire a better understanding of ailments and develop better therapies.

However, these data may be kept on external cloud storage offered by third-party service providers, which introduces possible security risks such as data leaking. This is because once the information is outsourced, neither the patients nor the physicians have control over it. In such a setting, the confidentiality and safety of this outsourced data should be preserved. For example, some medical institutions gather and maintain a huge number.

Literature Survey

M Abdalla has talked about We detect and close several gaps in public-key encryption in conjunction with a keyword search (PEKS) consistency (the degree to which false positives are created). We describe computational and statistical relaxations of the existing idea of perfect consistency, demonstrate that Boneh et al.'s scheme in Eurocrypt 2004 is computationally consistent, and propose a new statistically consistent scheme. We also offer a changeover from a safe PEKS scheme to an anonymous IBE scheme that, in contrast to the earlier one, ensures consistency. Finally, we propose three extensions to the fundamental concepts discussed here: anonymous public-key encryption with momentary keyword search, HIBE, and identity-based encryption with keyword search.

Blaze, Bleumer, and Strauss (BBS) introduced atomic proxy re-encryption in 1998, in which a semi-trusted proxy turns a ciphertext for Alice into a ciphertext for Bob without exposing the underlying plaintext. We believe that rapid and safe re-encryption will gain popularity as a solution for managing encrypted file systems. Despite being computationally efficient, widespread implementation of BBS re-encryption has been hampered by significant security problems. We offer novel re-encryption schemes that realise a stronger sense of security, and we illustrate the use of proxy re-encryption as a technique of adding access control to a secure file system, building on the work ofDodiandIvan.Our experimental file system's performance tests show that proxy re-encryption may be used efficiently in practise.

The open key protection with keyword exploration (PEKS) technique described by Boneh, Di Crescenzo, Ostrovsky, and Persiano allows one to search for encrypted keywords while maintaining the original data's security. We address two critical difficulties of a PEKS scheme in this research: "removing secure channel" and "refreshing keywords," which were not addressed in Boneh et al.'s study. We highlight the original PEKS scheme's inefficiency owing to the utilisation of the secure channel. We tackle this problem by developing an efficient PEKS technique that eliminates the need for a secure channel.

We then claim that when keywords are employed often in the PEKS scheme, caution must be given because this condition may contradict the security of PEKS.

A K Verma described how cloud computing gives multiple stakeholders/shareholders in the e-healthcare business universal access to a pool of shared resources. The rapid popularity of cloud computing has obviously sparked worries about the security of outsourced data. Due to the constrained resources of mobile devices, security solutions must perform compute extensive operations on the horizon for deployment. Traditionally, any change to an uploaded record would force the mobile client to re-encrypt and compute the hash value. We want to present in this study a pairing free incremental proxy re-encryption system without certificates that would run proportionate to the number of updates in time rather than the document length for improvement in file modification duties. The suggested method significantly improves on the file modification mechanism in relation to energy usage and turnaround timer. The suggested strategy was validated using a formal technique and the Z3 solver.

T Bhatia discussed that Access to personal health records is widespread and quick, allowing clinicians to make vital choices and save lives. Cloud computing has the ability to give ubiquitous and on-demand rapid entry to a common pool of resources and services to numerous stakeholders in the electronic healthcare business, such as patients, healthcare professionals, insurance companies, and so on. The rapid expansion and acceptance of cloud computing in electronic healthcare systems has naturally sparked worries about the protection of outsourced data. In this study, cryptanalysis of Qin's system is conducted, hence violating their scheme's anonymity.

We also suggested a single-hop unidirectional certificateless proxy re-encryption technique based on elliptic curves for safe sharing of mobile personal health records with public clouds that is suitable for low-power mobile devices. In certificateless proxy re-encryption, patients encrypt their information with public keys before sending it to the cloud, and the cloud resident semi trusted proxy re-encrypts it into cipher-text using the intended recipient's public key without being aware of the contents of the encrypted message. In the random oracle model, we prove its security. via formal analysis against a selected ciphertext attack. In compared to existing systems, our suggested method is more efficient and ideal for low-power mobile devices.

Existing Model

Yasnoff presented an e-healthcare storage structure that would avoid the possibility an individual infiltration causing the loss of a whole centralised dataset while preserving decent search speed.

Yangg et al. presented a dependable, searchable, and privacy-preserving e-healthcare system based on searchable encryption to secure sensitive healthcare files on cloud storage and enable cloud servers to search using encrypted data under patients' authority.

Boneh et al. developed the first PEKS architecture for an e-healthcare system in an open key environment. Later, Abdalla et al. examined the PEKS paradigm and created the consistency concept.

Baeketal. expanded PEKS to eliminate secure pathways between a user and the cloud server, allowing patients to connect with doctors on a safe basis.

While encryption protects data secrecy and may be used to solve data privacy issues as well as thwart assaults from rogue users and cloud services, it also causes user frustration. Traditional encryption approaches, for example, make it impossible to query this encrypted data since the ineffective information retrieval methods based on plaintext.

Given a lack of fast information retrieval mechanisms and insufficient fine-grained access control, the existing e-healthcare system faces a significant security and efficiency problem. he current system also implies that doctors must be available at all times. Medical care would be impossible if the doctor was unavailable.

However, a large majority of present CPRE schemes cannot ensure the privacy of the condition, which also contains some sensitive information.As opposed to that, if a malicious user can tell the difference between a re-encrypted ciphertext and an original ciphertext, the danger to safety increases since the bad user knows Alice is not available right now.

The present system approaches for retrieving information from encrypted PHRs remain a difficult task, particularly when working with vast amounts of data at a fine-grained level.

Unfortunately, no existing systems allow both encrypted keyword search and condition hiding the same time in practise, limiting the commercial applicability of proxy re-encryption in the e-healthcare system.

Proposed Methodology

To solve the challenges of inefficiency and condition privacy in the e-healthcare system, we present a proxy-invisible condition-hiding proxy re-encryption strategy with keyword search. Encryption is thought to be a simple and effective way to ensure data secrecy, but it also makes searching for encrypted data exceedingly complex. Searchable encryption technology enables the search of encrypted data without decryption, hence resolving the issue that users cannot manage remotely due to data encryption. As a result, searchability is required in the e-healthcare system. We want to develop an efficient, searchable, and privacy-preserving e-healthcare system in our suggested system.

In order to prevent privacy disclosure, we generate a conditional re-encryption by embedding a trapdoor in the re-encryption key to ensure the cloud server can only convert ciphertext under the designated condition. Moreover, the cloud server is responsible for storing the secret information, and providing keyword search services and also acts as a proxy to performre-encryption for data users.

When a keyword search request with a trapdoor is received from B, the cloud server performs information retrieval over the secured PHRs. Finally, B can decrypt ciphertext by utilising just his personal key to obtain specific medical information.

Data security: all patient data is encrypted before being submitted for cloud storage server. This protects data privacy and secrecy because The cloud server is unable to decipher any data from the encrypted PHRs.

Conditional authorization: If the doctor-in-charge (Alice) is absent, our system allows the duty to be delegated to another doctor (Bob) through a cloud server without the need to decrypt the PHRs, reducing information exposure up in the clouds server.

Condition-hiding: Our approach not only ensures the secrecy of patients' PHRs through encrypted data, but it also protects the secrecy of the condition encoded in the re-encryption key.

In our method, the authorised doctor (Bob) or a malicious user cannot tell which ciphertext is delivered to the de-legatee and which ciphertext gets re-encrypted by the cloud to whom Alice has delegated.

Collusion resistance: Even if a dishonest proxy colludes with Bob, Alice's private key remains secure under our scheme.

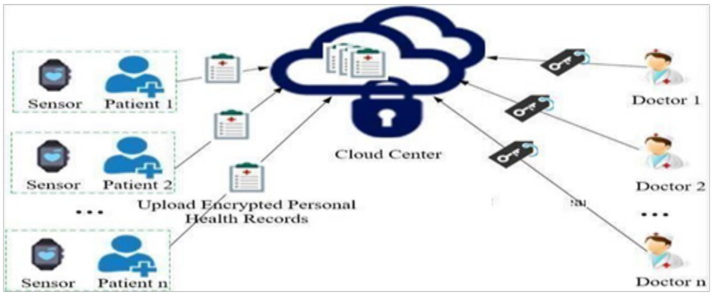

Figure 1 Proposed Architecture

Implementations

Patient

In the initial component, we create the Patient module, where a new patient is registered by filling out a registration form with their information. Once registered, the patient is unable to use the system. Only once the cloud server confirms the patient can they connect into the system; this is done to avoid unwanted users and to function as a security layer for the system. This module is in charge of managing patients' personal healthcare records (PHRs) and giving access to the information the patient has submitted. It gathers PHRs from various devices, encrypts them, and uploads them into a safe cloud server.

The patient should input their information, including Blood Group, Temperature, and Blood Pressure, to the patient module. Every patient To minimise duplication, each patient is assigned a unique patient ID.

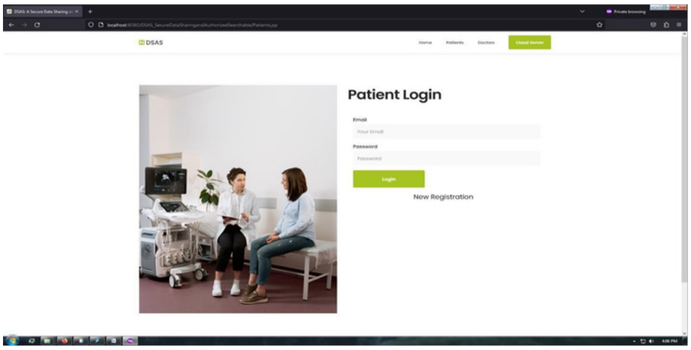

Figure 1.2 Patient Login Form

Doctor

In this module, we develop the Doctor's part, where the new doctor is registered by entering their details in the registration form. Once after registration the doctor cannot able to login in to the system similar to the earlier module.

Only if the cloud server approves the doctor only they can login into the system, this is developed to make the system more secure.

The doctor module provides authorized doctors with access to patients' PHRs. It allows them to search for patients available securely and ensure the confidentiality of the PHRs.

It stores the encrypted PHRs and handles requests for data retrieval. We have used Drive-HQ cloud service provider for the portion of the cloud where files are stored. cloud server in this module is built with the responsible to approving or rejecting both the patients and doctors also to make the system secure. The online server is responsible for assigning a patient to the doctor.

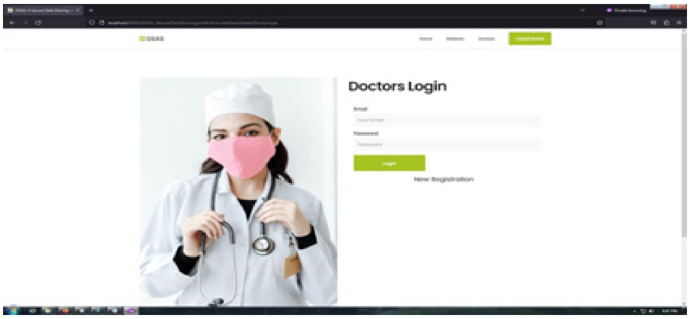

Figure 1.3 Doctors Login

Data Collection and Encryption

This component is in charge of gathering PHRs from different patients and encrypting them before uploading to the cloud server with them. Additionally, it keeps the PHRs' confidentiality, integrity, and availability by enforcing security rules.

Data Retrieval Phase

The information collection component is in charge of handling demands for health records from licenced physicians. The doctor module receives the relevant data from the cloud server, decrypts it, and then it delivers it back. They are only able to access the information if specific decryption key is available; otherwise, the data cannot be accessed. The key will not for all entities to share the same file. As a result, even if one entity leaks the key, the file remains safe and cannot be viewed.

Conditional Authorization

The DSAS project's primary module provides a secure and practical proxy searchable re-encryption mechanism for efficient and safe remote PHRs monitoring and investigation. It enables Alice (the doctor-in-charge) to delegate medical research and utilisation to Bob (the doctor-in-agent) via the cloud server, hence limiting information exposure to the cloud server.

Cloud Server

The cloud server module acts as an intermediary between the patient and doctor modules.

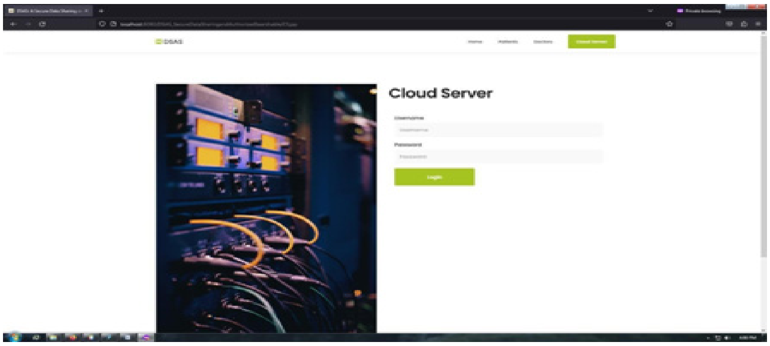

Figure 1.4 Cloud Server

Result

We introduced a proxy-invisible condition-hiding proxy re-encryption strategy that allows keyword search in this work, which may be used to secure data exchange and delegation in e-healthcare systems. With our new approach, a doctor named Alice (delegator) can create a conditional authorisation for a doctor named Bob (de-legatee) by supplying a re-encryption key. The cloud server can utilise the re-encryption key to conduct ciphertext transformation so that Bob can access the PHRs that were originally encrypted with Alice's public key, enabling safe delegation. The cloud server may search encrypted PHRs on the doctor's behalf without learning anything about the term or the underlying problem. In particular, we accomplished proxy-invisibility in the system.

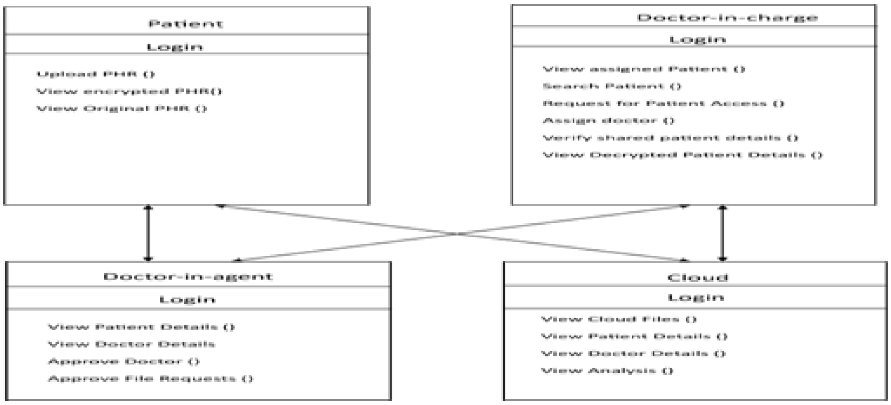

Figure 1.5 Result of the Project

Conclusions

We introduced a proxy-invisible condition-hiding proxy re-encryption strategy that allows keyword search in this work, which may be used to secure data exchange and delegation in e-healthcare systems. With our new approach, a doctor named Alice (delegator) can create a conditional authorisation for a doctor named Bob (de-legatee) by supplying a re-encryption key. The cloud server can utilise the re-encryption key to conduct ciphertext transformation so that Bob can access the PHRs that were originally encrypted with Alice's public key, enabling safe delegation. The cloud server may search encrypted PHRs on the doctor's behalf without learning anything about the term or the underlying problem. In particular, we accomplished proxy-invisibility in the system.

We also got the feature of collusion-resistance in the system, thus even if an individual dishonest cloud server colludes with the de-legatee (Bob), a delegator's (Alice) private key remains secure. We showed security with a rigorous proof, and performance study shows that our proposed system DSAS is efficient and practical.

Future Work

Here are Some Potential Career Paths

Scalability

The existing DSAS system solution is appropriate for small-scale deployments. Future development might concentrate on enhancing the system's scalability to accommodate large-scale e-healthcare systems with a high volume of patients and medical information.

Privacy Protection

While the DSAS system offers a high standard of privacy and security, there is always potential for development. Future research can concentrate on creating more robust privacy-protection strategies to ensure that patients' personal healthcare records are safeguarded even in the event of a breach or assault.

Usability

While the DSAS system is efficient and practical, it may be enhanced in terms of usability. Future work might concentrate on creating a user-friendly interface for physicians and patients to access and maintain PHRs, making it easier to use and lowering the risk of human error.

Interoperability

E-healthcare systems may incorporate many institutions and organisations using various software and hardware. Future work might concentrate on guaranteeing interoperability across various e-healthcare systems and facilitating easy exchange of encrypted PHRs among different providers.

Integration with Emerging Technologies

To improve functionality and security, the DSAS system may be combined with emerging technologies like as blockchain, AI, and IoT. Blockchain, for example, may be used to establish a decentralised, tamper-proof database for storing PHRs, whereas AI can do the same.

Adoption and Implementation

Finally, future study may focus on promoting the DSAS system's adoption and implementation in real-world e-healthcare systems. Collaboration with healthcare providers, lawmakers, and regulatory agencies may be required to guarantee that the system satisfies legal and ethical criteria while being compatible with existing healthcare systems.

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 encryptionrevisited: Consistency properties, relation to anonymous IBE, and extensions,'' in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005, pp. 205222.
2. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy re-encryption schemes with applications to secure distributed storage,'' ACMTrans. Inf. Syst. Secur., vol. 9, no. 1, pp. 130, 2006.
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.
4. T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy reencryption for e-healthcare data sharing in mobile cloud computing,'' Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520, Mar. 2020.
5. T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personal healthcare records using certicateless proxy re-encryption in cloud,''Trans. Emerg.Telecommun.Technol., vol. 29, no. 6, p. e3309, Jun. 2018.
6. I. F. Blake, G. Seroussi, and N. Smart, ``Advances in Elliptic CurveCryptography (London Mathematical Society Lecture Note Series (317)),vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666.
7. M. Blaze, G. Bleumer, and M. Strauss, ``Divertible protocols and atomicproxy cryptography,'' in Advances in Cryptology-EUROCRYPT. Berlin,Germany: Springer, 1998, pp. 127144.
8. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ``Publickey encryption with keyword search,'' in Proc. Int. Conf. Theory Appl.Cryptograph. Techn. Berlin, Germany: Springer, 2004, pp. 506522.
9. D. Boneh and B. Waters, ``Conjunctive, subset, and range queries onencrypted data,'' in Proc. Theory Cryptogr. Conf. Berlin, Germany:Springer, 2007, pp. 535554.
10. H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authentication as an intelligent process,'' IEEE Trans. Commun., vol. 67, no. 3,pp. 22602273, Mar. 2019.
11. H. Fang, L. Xu, and X. Wang, ``Coordinated multiple-relays basedphysical-layer security improvement: A single-leader multiple-followersStackelberg game scheme,'' IEEE Trans. Inf. Forensics Security, vol. 13,no. 1, pp. 197209, Jan. 2018.

12.L. Fang, W. Susilo, C. Ge, and J. Wang, ``Chosen-ciphertext secureanonymous conditional proxy re-encryption with keyword search,'' Theor.Comput. Sci., vol. 462, pp. 3958, Nov. 2012.
13.L. Fang, J. Wang, C. Ge, and Y. Ren, ``Fuzzy conditional proxy re-encryption,'' Sci. China Inf. Sci., vol. 56, no. 5, pp. 113, May 2013.
14.J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserving highorder bi-Lanczos in cloud-fog computing for industrial applications,'' IEEE Trans. Ind. Informat, early access, May 28, 2020, doi:10.1109/TII.2020.2998086.
15.J. Feng, L. T.Yang, Q. Zhu, and K.-K.-R.Choo, ``Privacy-preserving tensordecomposition over encrypted data in a federated cloud environment,''IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 857868,Jul. 2020.