JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Securing Data in Health Care Using Searchable Encryption

Mr.K. SIVA PRASAD (M.C.A). Mr.K. SIVA PRASAD *Mr. C. Hrishikesava Reddy (MTech, Ph.D). Rajeev Gandhi

Memorial college Of Engineering and Technology, Nandyal

Abstract

An increasing number of patients in the e-healthcare system can obtain top-notch medical services by sharing encrypted personal healthcare data (PHRs) with doctors or institutions involved in medical research. However, one of the main issues is that encrypted PHRs make it impossible to conduct efficient information searches. cutting back on the data usage. Another issue is that delivering medical care requires a doctor to be constantly accessible online, which may be too expensive for some professionals to afford (for example, to occasionally be absent). In this work, a brand-new, useful, secure proxy searchable re-encryption method is developed, allowing medical professionals to monitor and conduct research on patient health records remotely in an efficient and secure manner. Our DSAS scheme ensures the privacy and secrecy thanks to the following features: the doctor-in-charge, Alice, has the ability to delegate medical choices. These characteristics of PHRs ensure that patient healthcare records gathered by the devices are encrypted before uploading to the cloud server. Only authorized doctors or research institutes have access to PHRs. The cloud server limits the accessibility of information since Bob (the doctor-in-agent) or a certain research institution can utilize it for study. We formalize the idea of security and show the security of our system. Finally, performance analysis shows how effective our plan.

Key Words: Mobile healthcare sensor networks, proxy re-encryption, proxy invisibility, and searchable encryption.

1. INTRODUCTION

1.1 Introduction

Currently, e-healthcare sensor networks have developed to the point that they can be accepted and used on a broad commercial scale thanks to the swift rise of wearable technology, sensors, and artificial intelligence. The benefits of a mobile platform supported by an e-healthcare sensor network for patients looking for efficient and excellent medical care have been demonstrated. Patients' devices with sensors collect a lot of information about their medical histories, which helps doctors make more accurate diagnoses. You will be able to meet the patients' needs by using this data. Additionally, analysts and researchers in the field of medicine may use such data to do analytics to better understand diseases and create more potent treatments. However, these data may be retained in the cloud storage of third-party service providers [10], [16], or [34], which I ncreases security threats such as data leakage. This is because when the data is contracted out, neither patients nor medical professionals have access to it. This suggests that in such a setting, the privacy and security of this outsourced data should be protected. For instance, certain healthcare facilities amass large numbers of PHRs, store them on cloud servers, and grant the CDC access to use them (CDC). To help with illness prevention and control, doctors at the CDC are allowed to utilize data mining tools to examine this data. However, the CDC will inevitably divulge private patient information when collecting case information from medical facilities using typical data mining approaches. A significant challenge is determining how to store and retrieve PHRs properly. The e-healthcare system mandates more security and privacy protections for practices in terms of data and access to data. PHRs should all be encrypted before being saved in the cloud to prevent the information from leaking out [11], [14], [15], [26], [27], [42]-[44]. The user experience can suffer from encryption, even while it offers data security, can be used to address privacy concerns, and guards against attacks from malicious users and cloud servers. For example, because of the ineffective It is challenging to query this encrypted data using information retrieval techniques based on plaintext, conventional encryption algorithms [28]. As a result, most research makes use of the searchable encryption (SE) cryptosystem to get beyond the constraints of the conventional approaches. Patients employ searchable encryption technology with the e-healthcare system to first encrypt the potential keyword as an index before uploading it to the cloud server with the encrypted PHRs. An authorized doctor or research institution can employ encrypted keyword search by sending a trapdoor created with a certain term to the cloud server.

2. Literature Survey

• **[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,2005 :**, Using PEKS, we identify and close many holes in the consistency of the generation of false positives for public-key encryption. We present a new statistically consistent scheme, demonstrate the computational consistency of the scheme, and discuss relaxations of the notion of complete consistency in terms of computing and statistics. In addition, we offer a safe PEKS scheme that, in contrast to the prior one, guarantees consistency when converting from a single anonymous IBE scheme. Our final three suggestions are identity-based encryption with keyword search, public-key encryption with temporary keyword search, and anonymous HIBE. Our last recommendations are these three enhancements to the core concepts we've been talking about here. We present a unique statistically consistent scheme, demonstrate the scheme's computational consistency, and address relaxations of the idea of perfect consistency in terms of statistics and computing. We also provide a safe PEKS scheme that, unlike the previous one, ensures consistency when converting from a single anonymous IBE scheme.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ‘‘Improved proxy re-encryption schemes with applications to secure distributed storage: We provide several secure proxy re-encryption techniques that perform better than earlier approaches. The main advantages of our systems are that they are unidirectional (i.e., Alice can delegate to Bob without Bob having to delegate to her) and that delegators are not required to reveal all of their secret key information. This enables a proxy to re-encrypt ciphertexts without the need to interact with the delegate or even reveal the ciphertexts. Our solutions only use a small amount of the trust in the proxy. Our methods have two fundamental benefits: they are unidirectional (Alice can delegate to Bob without Bob needing to delegate to her), and delegators are not compelled to reveal all of their secret key information. This As a result, a proxy can re-encrypt the delegators' ciphertexts without the delegators having to divulge them.

3. OVERVIEW OF THESYSTEM

3.1 Existing System

Blockchain technology offers a decentralized, secure method of storing and distributing patient health data in the current system. It guarantees that all transactions are recorded on an immutable ledger and gives patients choice over who has access to their data.

3.1.1 Disadvantages of Existing System

Time consuming.

Dependence on technology.

Lack of flexibility

3.2 Proposed System

A strong permission and authentication mechanism is required in the proposed system to guarantee that only authorized users can access patient data. Password-based authentication, two-factor authentication, or biometric authentication can all be used to accomplish this.

3.3 Methodology

In this project works on these modules

BOB:

Register: Bob has to sign up by providing their username, password, email, contact information, home address, birthdate, and pin code.

Login: He must use their current login information.

Search & decrypt patient details: The Bob needs to look and wants to decipher the patient's information.

Logout: Finally, the bob must Logout.

Alice:

Register: Alice wants to sign up with a username, password, contact information, address, email, date of birth, and pin code.

Login: Alice will need to enter their username and email to log in.

Upload file: Alice needs to upload the patient's file for the next check.

View all datasets: Alice is required to examine every dataset used in the project.

View all attacks: Alice has access to the count of assaults.

Logout: Finally, the user who logged in has to log out.

Cloud server:

Login: Users can sign in to the cloud server using their username and email.

User authorization: The person in attendance has to authorize with the cloud server.

Owner authorization: In this case, the owner will also need to request authorisation from the cloud server.

View all datasets: All of the datasets used in this study are available on the cloud server.

View disease results: The patient's disease findings can be seen on the cloud serve.

View attacker results: The findings of the patient whose disease was addressed by the patient may then be seen on the cloud server.

Logout: When the entire job is done, the cloud server must logout.

4 Architecture

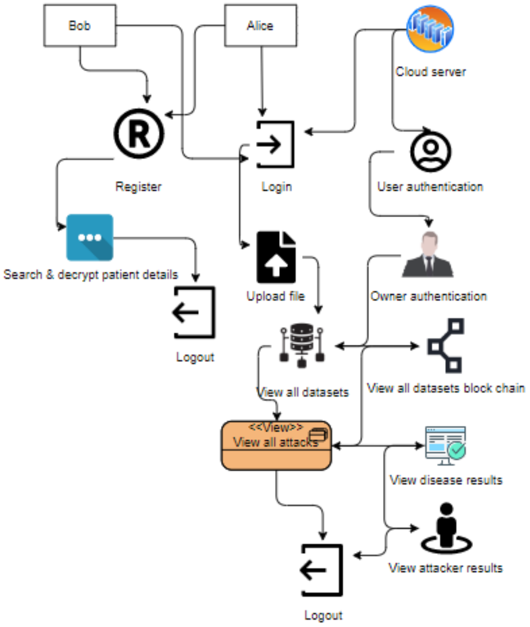
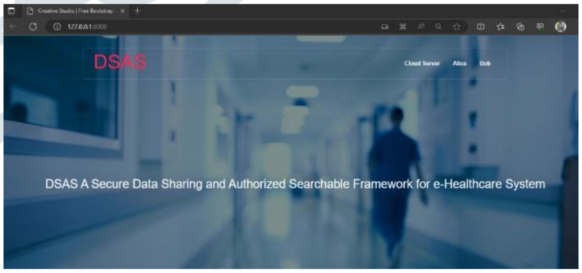


Fig 1: Frame work of proposed method

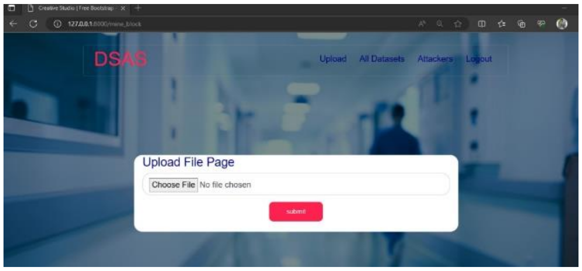
5 RESULTS SCREEN SHOTS

Home Page:



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

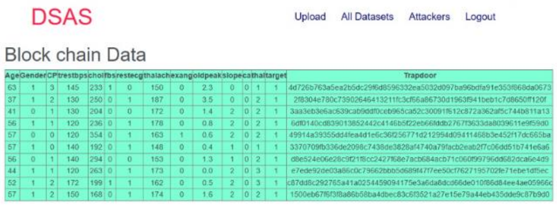
Upload Data:



Upload File Page

No file chosen

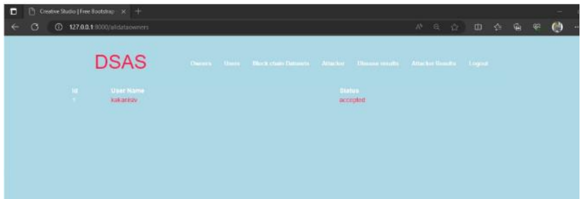
Tap door :



Block chain Data

Age	Gender	CP	trestbps	chol	fbs	restecg	thalach	exang	oldpeak	slope	ca	thal	target	Trapdoor
63	1	3	145	233	1	0	150	0	2.3	0	0	1	1	4d726b763a5ea2b5dc29f6d8596332ea5032d097ba96bdfa91e353f868da0673
37	1	2	130	250	0	1	187	0	3.5	0	0	2	1	2f8304e780c7390264641321 1fc3cf66a86730d1963f941beb1c7d8650ff120f
41	0	1	130	204	0	0	172	0	1.4	2	0	2	1	3aa3eb3e6ac639cab9ddf0ceb965ca52c30091f612c872a362af5c744b811a13
56	1	1	120	236	0	1	178	0	0.8	2	0	2	1	6df0140cd839013852442c4146b5f22eb66fddb2767f3633da8039611e9f59d0
57	0	0	120	354	0	1	163	1	0.6	2	0	2	1	49914a39355dd4fea4d1e6c36f256771d212994d09411468b3e452f17dc665ba
57	1	0	140	192	0	1	148	0	0.4	1	0	1	1	3370709fb336de2098c7438de3828af4740a79facb2eab2f7c06dd51b741e6a6
56	0	1	140	294	0	0	153	0	1.3	1	0	2	1	d8e524e06e28c9f21f8cc2427f68e7acb684acb71c060f99796dd682dca6e4d9
44	1	1	120	263	0	1	173	0	0.0	2	0	3	1	e7ede92de03a86c0c79662bbb5d689f47f7ee50cf7627195702fe71ebe1df5ec
52	1	2	172	199	1	1	162	0	0.5	2	0	3	1	c87dd8c292765a41a0254459094175e3a6da8dcd66de010f66d84ee4ae05966c
57	1	2	150	168	0	1	174	0	1.6	2	0	2	1	1500eb67f6f3f8a86b58ba4dbec83c6f3521a27e15e79a44eb435dde9c87b9d0

Result:



id	User Name	Status
1	kakanisiv	accepted

7. CONCLUSION

✓ The keyword search functionality and data interchange and delegation security features of the proxy-invisible condition-hiding proxy re-encryption system we developed in this study may be applied in e-healthcare systems. By giving a re-encryption key under our new approach, a doctor named Alice (the delegitimate) can generate a conditional authorization for a doctor named Bob (the delegate). Because the cloud server can conduct ciphertext transformation using the re-encryption key, enabling secure delegation, Bob may now access the PHRs that were initially encrypted using Alice's public key. Without knowing the phrase or the underpinning lying scenario, the cloud server may scan encrypted PHRs on the doctor's behalf. We particularly achieved the proxy-invisible property of the system. We have also identified the collusion-resistance property of the system, which guarantees that Alice's private key will be secure even if a dishonest cloud server colludes with the delegate (Bob). Rigorous evidence has established the security of our suggested system, DSAS, and performance analysis backs up its efficacy.

8. 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. 205–222.

[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. 1–30, 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. 1249–1259.

[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.

[5] T. Bhatia, A. K. Verma, and G. Sharma, ‘‘Secure sharing of mobile personal healthcare records using certificateless 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 Curve Cryptography (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 atomic proxy cryptography,’’ in Advances in Cryptology-EUROCRYPT. Berlin, Germany: Springer, 1998, pp. 127–144.

[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: Springer, 2004, pp. 506–522.

[9] D. Boneh and B. Waters, ‘‘Conjunctive, subset, and range queries on encrypted data,’’ in Proc. Theory Cryptogr. Conf. Berlin, Germany: Springer, 2007, pp. 535–554.

[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. 2260–2273, Mar. 2019

.