Fortifying Facts in Health Caution Consuming Examine Encryption

[1]Name of 1st Mr Gaurav Khatri
[1]Designation of 1st Assistant Professor
[1]Name of Department of 1st Faculty of Computer Science & Applications
[1]Name of organization of 1st Gokul Global University, Sidhpur, Patan, Gujarat – India

Abstract

Cutting back on the data usage. secure manner. These characteristics of PHRs ensure that patient healthcare records gathered by the devices are encrypted before uploading to the cloud server. The cloud server limits the accessibility of information since Bob (the doctor-inagent) or a certain research institution can utilize it for study.

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

INTRODUCTION

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. This is because when the data is contracted out, neither patients nor medical professionals have access to it. 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. 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]. As a result, most research makes use of the searchable encryption (SE) cryptosystem to get beyond the constraints of the conventional approaches. An authorized doctor or research institution can employ encrypted keyword search by sending a trapdoor created with a certain term to the cloud server.

Literature Survey

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H.
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.
We provide several secure proxy reencryption 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. of their secret key

information. This As a result, a proxy can re-encrypt the delegators' ciphertexts without the delegators having to divulge them.

OVERVIEW OF THESYSTEM

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.

Disadvantages of Existing System

Time consuming.
Dependence on technology.
Lack of flexibility

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.

Methodology

BOB:

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

Logout: Finally, the bob must Logout.

Alice:

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

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

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

Cloud server:

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

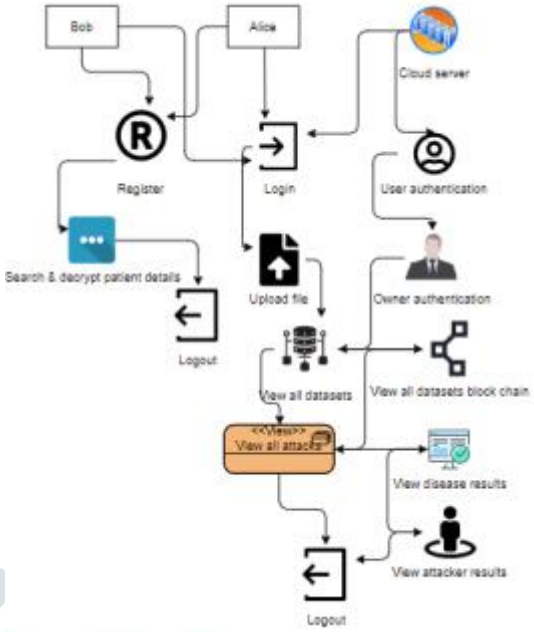
Owner authorization: In this case, the owner will also need to request authorisation from the cloud server.

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.

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

Architecture



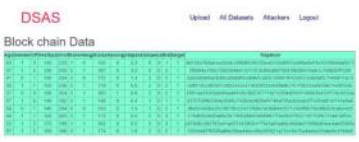
Frame work of proposed method

RESULTS SCREEN SHOTS

Home Page:

Upload Data:

Tap door:



Result:

CONCLUSION

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. 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.

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 reencryption 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. 2017.
[5] T. Bhatia, A. K. Verma, and G. Sharma, ‘‘Secure sharing of mobile personal healthcare records using certificateless proxy reencryption in cloud,’’ Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. e3309, Jun. 2017.
[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 CryptologyEUROCRYPT. 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. 2016