www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

SAFE HEALTH DATA SHARING: A METHOD FOR PROTECTING YOUR MEDICAL RECORDS

[1] Mrs. D. Keerthi Reddy,[2] T. Pooja,[3] Y. Suma,[4] R. Vinay Reddy,[5] Sk. Kalesha
[1]Assistant Professor,[2345]B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

The widespread acceptance of cloud-based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs. Therefore, we propose a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced

to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High-Level Petri Nets (HLPN).

Performance evaluation regarding time consumption indicates that the SeSPHR methodology has potential to be employed for securely sharing the PHRs in the cloud.

I. INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

How Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling: The provider's computing

Index in Cosmos
JUNE 2025, Volume 15, ISSUE 2
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

II. LITERATURE SURVEY

TITLE: Public key encryption with keyword search.

AUTHORS: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano

ABSTRACT: We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

TITLE: Verifiable attribute-based keyword search over outsourced encrypted data.

AUTHORS: Q. Zheng, S. Xu, and G. Ateniese

ABSTRACT: It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner's outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations. We formally define the security requirements of VA B K S and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable.

TITLE: Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions

AUTHORS: M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi.

ABSTRACT: We identify and fill some gaps with regard to consistency (the extent to which false positives are produced) for public-key encryption with keyword search (PEKS). We define computational and statistical relaxations of the

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

existing notion of perfect consistency, show that the scheme of [7] is computationally consistent, and provide a new scheme that is statistically consistent. We also provide a transform of an anonymous IBE scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally, we suggest three extensions of the basic notions considered here, namely anonymous HIBE, public-key encryption with temporary keyword search, and identity-based encryption with keyword search

TITLE: Anonymous hierarchical identity-based encryption (without random oracles).

AUTHORS: X. Boyen and B. Waters.

ABSTRACT: We present an identity-based cryptosystem that features fully anonymous ciphertexts and hierarchical key delegation. We give a proof of security in the standard model, based on the mild Decision Linear complexity assumption in bilinear groups. The system is efficient and practical, with small ciphertexts of size linear in the depth of the hierarchy. Applications include search on encrypted data, fully private communication, etc. Our results resolve two open problems pertaining to anonymous identity-based encryption, our scheme being the first to offer provable anonymity in the standard model, in addition to being the first to realize fully anonymous HIBE at all levels in the hierarchy.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

The widespread acceptance of cloud-based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs.

DISADVANTAGES

- Fragmented Data Storage: Existing systems often store health data in fragmented ways, with different healthcare providers maintaining their own records. This fragmentation can lead to incomplete patient profiles and difficulties in accessing comprehensive health information in emergencies.
- Limited Interoperability: Healthcare systems may use incompatible technologies and data formats, making it challenging to share medical records seamlessly between different hospitals, clinics, and healthcare providers. This can hinder the continuity of care.
- Security Vulnerabilities: Despite efforts to protect medical records, existing systems can be susceptible to security breaches and cyberattacks. These breaches can compromise patient confidentiality and result in the unauthorized access or theft of sensitive health data.

PROPOSED SYSTEM

We propose a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi- trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore

ADVANTAGES

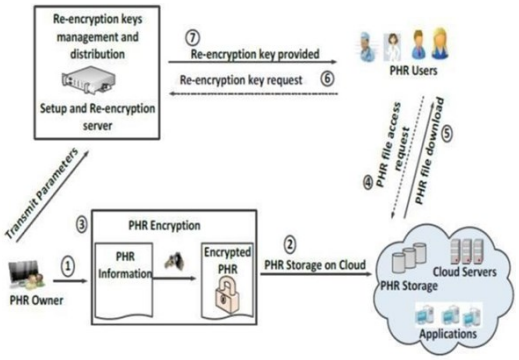
- Enhanced Data Interoperability: The proposed system would prioritize data standardization and interoperability, ensuring that health records can be seamlessly exchanged between different healthcare providers and systems. This would improve the continuity of care and reduce fragmentation in patient data.
- Granular Patient Consent Control: The proposed system would empower patients with granular control over their health data. Patients can specify who can access their

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

records, for what purposes, and for how long. This level of control ensures that data sharing only occurs with informed and explicit patient consent.

- Immutable Data with Blockchain: Implementing blockchain technology in the proposed system would provide an immutable ledger of health data transactions. This would enhance security by making it extremely difficult for unauthorized parties to tamper with or alter patient records, ensuring the integrity of the data.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

MODULES

- Cloud
- User
- Setup and Re-encryption Server

MODULE DESCRIPTION

- **Cloud:**

The scheme proposes the storage of the PHRs on the cloud by the PHR owners for subsequent sharing with other users in a secure manner. The cloud is as-sumed as un-trusted entity and the users upload or download PHRs to or from the cloudservers. As in the proposed methodology the cloud resources are utilized only to upload and download the PHRs by both types of users, therefore,no changes pertaining to the cloudare essential.

- **Setup and Re-encryption Server (SRS):**

The SRS is a semi-trusted server that is responsible for setting up pub-lic/private key pairs for the users in the system.The SRS also generates the re-encryption keys for the purpose of secure PHR sharing among different user groups. The SRSin the proposed methodologyis considered as semi-trustedentity.Therefore,we assume it to be honestfol-lowing the protocol generallybut curious in nature. The keys are maintained by the SRS but the PHR data is never transmitted to the SRS. Encryption and decryption opera-tions are performed at the users' ends. Besides the key management, the SRS also implements the access control on the shared data.

The SRS is independent server that cannot be deployed over a public cloud because of cloud being un- trusted entity. The SRS can be maintained by a trusted third-party organization or by a group of hospitals for convenience of the patients.It can also be maintained by a group of connected patients. However, SRS maintained by hospitals or by a group of patients will generate more trust due to involvement of health professionals and/or self-control over SRS by patients.

- **Users:**

Generally, the system has two types of users:(a)the patients(owners of the PHR who want to securely share the PHRs with others) and (b)the family members or friends of patients, doctors and physicians, health in-surance companies' representatives, pharmacists, and researchers. In SeSPHR methodology, the friends or fami-ly members are considered as private domain users whereas all the other users are regarded as the publicdomain users. The users of both the private and public domain may be granted various levelsof access to the PHRs by the PHR owners. For example, the users that belong to private domain may be given full access to the PHR,whereas the public domain users,such as physicians, researchers, and pharmacists may be grantedac-cess to some specific portions of the PHR.. Inother words, the SeSPHR methodologyallowsthe patients to exercise the fine-grained access control over the PHRs. All of the users in the system are required to be registered with the SRS to receive the services of the SRS.

V. SCREENSHOTS

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

FIG 1 : HOME PAGE

FIG 2: CLOUD SERVER LOGIN

FIG 3 : CLOUD SERVER WELCOME PORTAL

FIG 4 : ACCESS CONTROL

FIG 5: AUTHORIZE DOCTOR

FIG 6: KEY REQUEST

FIG 7: KEY TRANSACTIONS

VI. CONCLUSION

CONCLUSION

We proposed a methodology to securely store and transmission of the PHRs to the authorized entities in the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access control to different portions of the PHRs based on the access provided by the patients. We implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re- encryption keys issued by a semi-trusted proxy are able to decrypt the PHRs. The role of the semi- trusted proxy is to generate and store the public/private key pairs for the users in the system. In addition to preserving the confidentiality and ensuring patient-centric access control over the PHRs, the methodology also administers the forward and backward access control for departing and the newly joining users, respectively. Moreover, we

formally analyzed and verified the working of SeSPHR methodology through the HLPN, SMT-Lib, and the Z3 solver. The performance evaluation was done on the on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time. The experimental results exhibit the viability of the SeSPHR methodology to securely share the PHRs in the cloud environment.

FUTURE SCOPE

Integration with emerging technologies:

- Explore integration with emerging technologies such as blockchain to enhance the security and immutability of medical records.Investigate the use of advanced encryption techniques and protocols to further strengthen the security of PHRs.
- Interoperability and standardization:Work towards establishing industry standards and interoperability protocols to ensure seamless integration with different e-Health systems.Collaborate with healthcare standards organizations to align the SeSPHR methodology with evolving standards for health data exchange.
- Scalability and Performance Optimization:Focus on optimizing the scalability and performance of the SeSPHR methodology to handle a growing volume of PHRs and increasing user demands
- User Authentication and Access Control: Enhance user authentication mechanisms, such as biometrics or multi-factor authentication, to add an extra layer of security.Implement fine- grained access control policies to ensure that only authorized individuals have access to specific portions of the PHRs.
- Regulatory Compliance:Keep abreast of evolving healthcare regulations and ensure that the SeSPHR methodology remains complaint with regional and international data protection laws.

REFERENCES

1. K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things," Future Generation Computer Systems, 85, 2018, pp. 190-200.
2. K. Gai, M. Qiu, and X. Sun, "A survey on FinTech," Journal of Network and Computer Applications, 2017, pp. 1-12.
3. A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user cen-tered approach, "Future Generation Computer Systems, vols. 43-44,pp. 99-109, 2015.
4. A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Sham-shirband, "Incremental proxy re- encryption scheme for mo-bile cloud computing environment,"The Journal of Supercom- puting,Vol. 68, No. 2, 2014, pp. 624-651.
5. R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-
6. Y. Song and L.-W. He, "Optimal rare query suggestion with implicit user feedback," in Proc. 19th Int. Conf. World Wide Web, 2010,pp. 901–910.
7. T. Miyanishi and T. Sakai, "Time-aware structured query suggestion," in Proc. 36th Int. ACM SIGIR Conf. Res. Develop. Inf.