Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 2326-2331

Research Article

UUBE for Secure Sharing of Personal Health Records in Cloud

Dr. Dhina Suresh[1]

[1]Assistant Professor, Department of Computer Science,St.Joseph's College of Arts and Science for WomenHosur, Tamilnadu, India
[1]dhinadulcy@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Cloud based Personal Health Record (PHR) is a prominent cloud based platform for switching a person's health information in a secure manner. They are next generation cloud platform making possible for well organized , reliable & scalable data access to foster the public care. There happen numerous security issues when records of the data owners are reevaluated through the outsider cloud suppliers. The health records which are kept secret should be put away and recovered through a protected source with no misfortune in the information. Nonetheless sharing and probing of the data is the bottom line, but when it is outsourced beyond doubt it is a burdensome task. It might prompt reveal the delicate data thus the records may get helpless against the technocrats. In this article, we have suggested a novel access control structure called as User Usage Based Encryption (UUBE) constructed on the searchable attribute based encryption to guarantee the data protection. Utilization is planned as credential with a time span to each private attribute. The client can decipher only if there is a match between the accreditation's related with the attributes. Utilizing the feature extraction the accessible encryption plot empowers a predictable directing of encoded credits. Prior to starting the encryption conspire we apply the singular value decomposition algorithm to the non-utilized or less utilized credits to diminish the trait set. Moreover the information client privacy traps are handled utilizing the semantic grouping. To save the client secrecy a solid overlay protection convention is planned. We show a total security investigation with the goal that our suggested framework rules the cutting-edge approaches regarding communication and encoding cost.

Keywords - Reliable, Scalable, Access Control, Searchable, Encryption, Singular Value Decomposition.

1. Introduction

The Electronic Health Record (EHR) System is enhancement of the individual well-being Record framework to work with a patient to make his own well-being data in one medical clinic and oversee or share the data with others in different emergency clinics. Many practical patient-centric EHR systems have been implemented such as Microsoft Health Vault (Microsoft) and Google Health (Google). It urges a patient to make, oversee and share his own well-being data with the assistance of the Cloud Service Provider.We realize that the client should present all his delicate data to the Cloud Service Provider.

The CSP's should guarantee security. Cloud based Personal Health Record (PHR) is a prominent cloud based platform for switching a person's health information in a secure manner. They are next generation cloud platform making possible for well organized , reliable & scalable data access to foster the public care. We have proposed an access control structure called as User Usage Based Encryption (UUBE) that falls under the accessible quality based encryption plot. It likewise invigorates the information security, fortifies the protection and and automatic user revocation. The use of the attribute is enciphered with the public key by the information proprietor.

To encourage the accessible encryption, the information proprietor can create a multitude set of keywords that can particularly distinguish the directive for explicit keyword re-search in the record. The client himself can proficiently foreordain the attributes which are to be searched automatically using the feature extraction algorithm.

Based on credential extracted by the cloud, cloud discloses the categorized information to the data user based on his credential and timeslot similarity for search request. Otherwise the search request will be terminated. In that way, the access rights of the data user will expire automatically in specified timeslot. This is the enables automatic delegation revoking based on timing in a searchable encryption system.

2. Literature review and related work

2.1. Multi Authority Attribute based Encryption

To achieve fine-grained and scalable data access control for PHRs, attribute based encryption (ABE) techniques is leveraged to encrypt each patient's PHR file based on the sensitive attributes (Li, Yu, Zheng, Ren, & Lou, 2013). The secure data outsourcing is focused on the multiple data owner scenario as to divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE.

2.2. Searchable Encryption for Keyword Search

The Searching of the relevant information in the encrypted record set will lead to malicious attack launch. An attacker is possibly to launch dictionary attacks or off-line keyword guessing attacks to exploit the hidden keywords in order to access the healthcare data record. Data owner preset the keywords for their record before performing the data encryption. In order to prevent the guessing attack, public key encryption is defined for the searchable encryption of the personal health record. The enhanced Security model for public key encryption scheme (Liu P. , Wang, Ma, & Nie, 2014) have been used to support multiple keywords or data user search function (Wang, Cao, Ren, & Lou, 2012).

2.3 Identity Based Encryption

The Identity Based Cryptosystem (Shamir, 1979) is an email-address based public-key infrastructure cryptographic system developed by Adi Shamir. It allows the user to generate a public key from a known identity value such as an ASCII string. The major drawbacks of IBE may be if the Private Key Generator (PKG) is weakened, the encrypted messages will be under risk and this causes the key management problem. As the private keys are in the hands of the PKG, he may decrypt or even sign any message without authorization.

2.4 Attribute Based Encryption

In the ABE (Sahai & Waters, 2005), (Pandey, Goyal, Sahai, & Waters, 2006) scheme with a set of descriptive attributes the cipher text and the keys are labeled. The message can be decrypted only if there is a match between the attributes of the cipher text and the attributes of the user.

3. OUTLOOK OF SECURE SHARING OF PHR'S IN CLOUD USING USER USAGE BASED ENCRYPTION

In this model of UUBE (Florence, Suresh 2019), data owner outsources their confidential personal health files to clouds server for effective retrieval by health care provider (Microsoft) and towards storage service which avoids incurring losses due to data management and maintenance in the local systems.

However, health care provider requires a medical record for medical processing as they demand record through search mechanism in the cloud. The proposed model is devised as a novel access control mechanism named as User Usage Based Encryption (UUBE) based on the Searchable Encryption (SE) scheme to ensure the robust privacy preservation. A Searchable Symmetric Encryption (SSE) scheme (Kamara & Papamanthou, 2013) is a collection of four polynomial-time algorithms as follows:

KeyGen(λ, s) : It is a probabilistic key generation algorithm that takes a security parameter λ, and outputs a secret key k. It is run by the user to setup the scheme.

BuildIndex(k, D) : It takes a secret key k and a health record collection D as inputs, and outputs an index I.

Trapdoor(k, w) : It is an algorithm that takes a secret key k and a set of keywords w as inputs, and outputs a trapdoor Tw.

Search(I, Tw) : It takes an index I and a trapdoor Tw for keyword w as input, and returns a search result D(w).

The proposed model is devised as a novel access control mechanism named as User usage based encryption (UUBE) (Suresh, Florence) based on the searchable encryption to ensure the robust privacy preservation. A searchable encryption (Zhang & Zhang, 2011) enables efficient routing of encrypted events using data or feature extraction algorithm. Searchable encryption is been associated with a trapdoor to keywords as depicted in fig 1 which is generated automatically by the data owner to enable the server to search activity while keeping keyword hidden. The proposed constraint on access control scheme would not leak anything beyond the outcome of the keyword in a search.

The Singular Value Decomposition (SVD) (Yinlai, Hayashi, & Wang, 2014) is applied to unused or less used attribute in order to dimensionally reduced feature set or attribute set before the encryption.

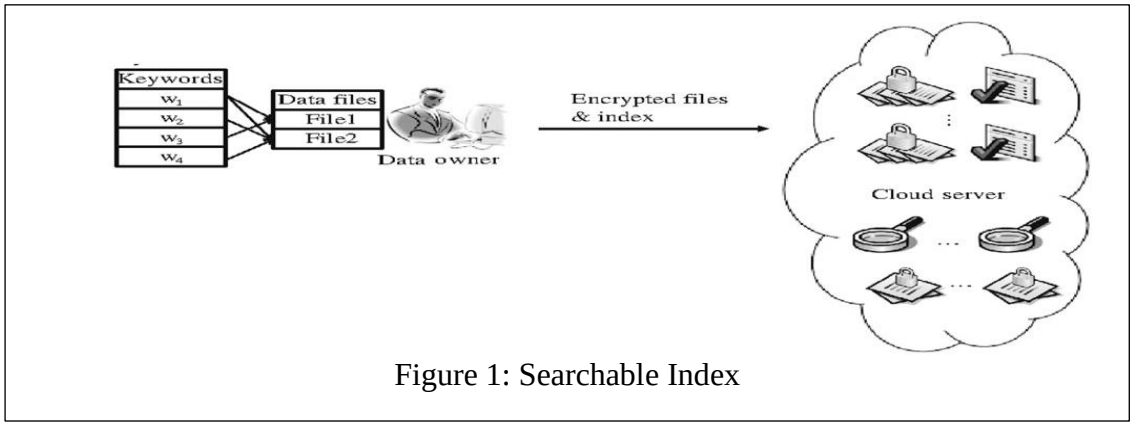


Figure 1: Searchable Index

4. Illustration of user usage based encryption algorithm

In the system, the PHR of the patients are encrypted by an asymmetric encryption algorithm named as Elliptic Curve Cryptography (Karakoyunlu, Gurkaynak, Sunar, & Leblebici, 2010). The algorithm focus on the searchable keyword encryption and the timing controlled data rendering function. The proposed model is resistant to key leakage attacks through the usage of ECC.

Setup (λ, S) → (PK, MK) : The setup algorithm takes as input the security parameter λ and an attribute universe description S. It gives the public parameters PK and the master secret key MK.

Attribute Generation algorithm defines the access structure and the attributes. Users U1, ..., Un with a set of attributes that are included in the A are authorized users and are allowed access to the data.

User List Generation algorithm takes as input Pk and the user identity ID and a time seal Ts. If the time seal does not match the user will be revocated automatically.

Policy Generation access methods are cryptographically encrypted to provide an access policy. The policy is generated along with the time seal (Ts). Time limits are specified for attribute revocation.

Key Generation is done with the generator G, time seal Ts and user attribute set AU = A1, ..., An where AU ∈S as input, the algorithm generates a key pair, a public key Pk known to all and a private key Sk kept secret for the particular user.

Building the Index with R1, ..., Rn as a set of health records. Let R1, ..., Rn be the input, using the feature extraction and feature selection algorithm as depicted in figure 2 a set of keywords are generated to form the index.

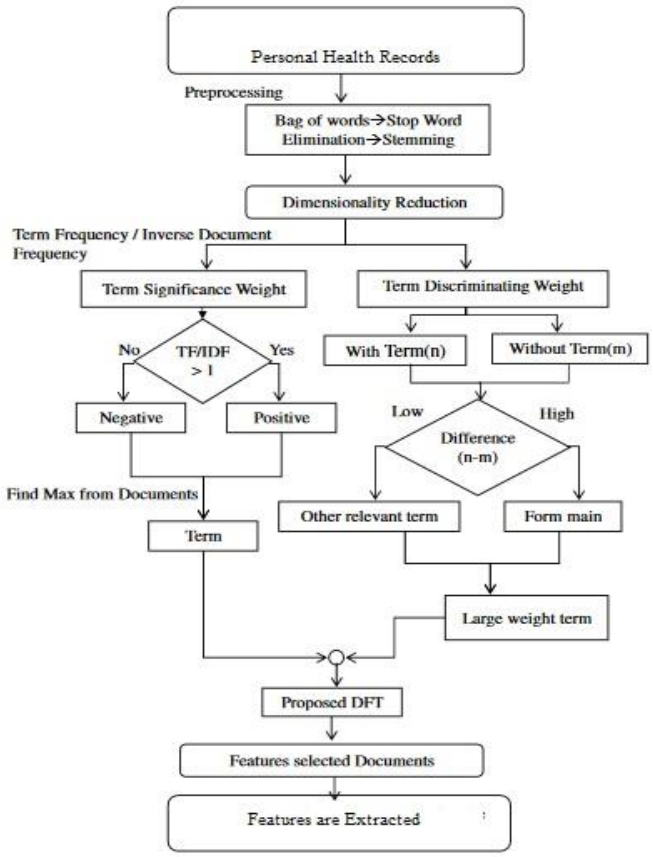
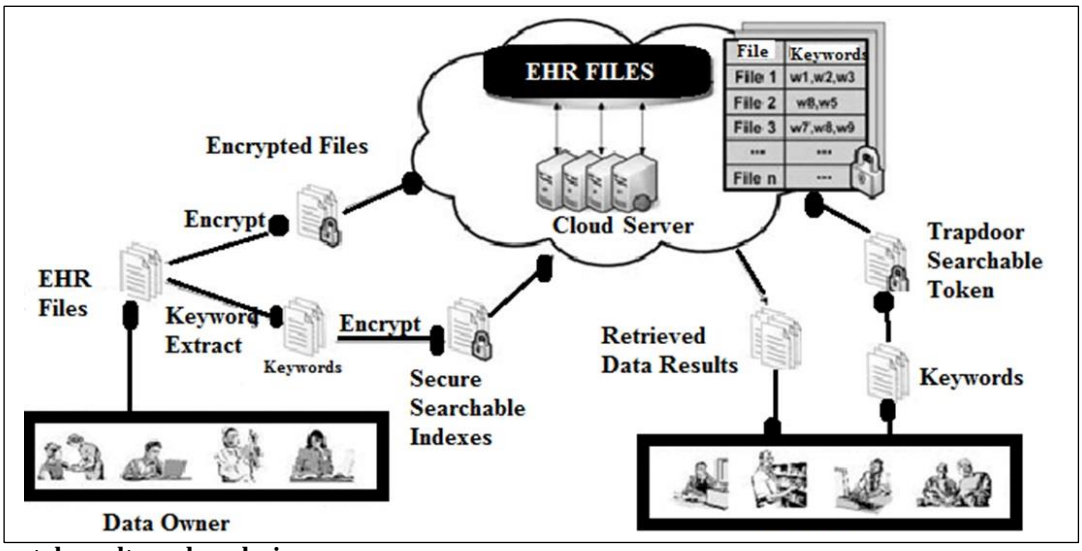


Figure 2: Feature Extraction Process

Encryption of data is done with Td, Pk, Ts, Ap, PHR as the input, the file is encrypted the file is stored in the Cloud Server.

Decryption process first searches using the search function Search(I, Td). Searching is performed on the secure Index I with the help of Td. The Attributes are mapped and grouping of the attributes is carried out. Decryption is done when the user enters any keyword. The private key of the user SK which contains the Time Seal Ts, Events(Attribute Set) A1, A2, ..., An are verified.



5. Experimental results and analysis

The comparative analysis between various traditional encryption algorithms and the proposed scheme for the parameters of encryption / decryption time and speed with the number of attributes conveys that the proposed scheme can effectively overcome the issues Lack of data integrity, Complexity in robust key generation, Computational Time, Collision resistence in encryption process, Data crashing, Communication Cost.

The average difficulty time (can also be called as average computing time) when compared between Multi Authority Atrribute based Encryption along with User Usage Based Encryption for Encryption (AvgET), Decryption (AvgDT), Collusion Resistance (CRTime) and User Revocation (URTime) for data size of 50 GB are given in table 1 and the same is depicted in figure 4. Proposed System is an effective approach to prevent the eavesdropping attacks over a cloud environment has it has strongly anonymized.

Technique	Encryption Time in (ms)	Decryption Time in (ms)	User Revocation (ms)	Collusion Resistance (ms)
User Usage based Encryption	158	144	4	9
Multi Authority – Attribute Based Encryption	294	272	9	15

Table 1: Performance Analysis for data size of 50 GB

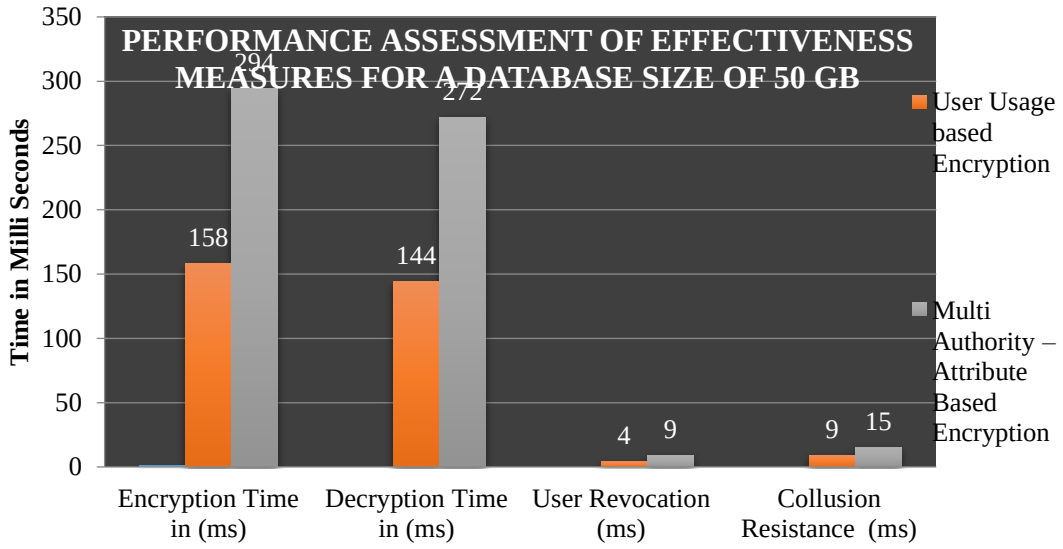


Figure 4: Performance Assessment of Effectiveness Measures for a Database Size of 50 GB

6. Conclusion and future work

The Securing of the health record in the cloud environment have considered through the implementation of the proposed scheme. The different models have integrated into the proposed scheme. Several journals have been published in this area using the methodology used in this research which is as follows The journal entitled as Enhanced Secure Sharing of PHR's in Cloud using User Usage Based Attribute Based Encryption and Signature with Keyword Search provides various information such as searchable encryption enable index generation and keyword formation for the familiar query. The searchable encryption also generates the trap door for the data user benefits.

In this Usage is mapped as a credential with a time-frame to every private attribute. In this data, user can decipher a fortified attribute only if there is a match between the credentials associated with the attribute. Additionally, Multi-Credential routing is applied to strengthen the confidentiality of the fragile records. One of the future directions is to combine other privacy preserving techniques with cryptographic techniques. Efficient access to request data access under crisis scenario can be empowered under break glass access phenomena. Biometric inclusion can be used for key generation process in the searchable technique.

References

A. Microsoft, h. v. (n.d.). http://www.healthvault.com
B. Google, h. (n.d.). https://www.google.com/health
C. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Transactions on Parallel & Distributed Systems , 24(1), 131-143.
D. Wang, C., Cao, N., Ren, K., & Lou, W. (2012). Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data. EEE Transaction on Parallel Distribributed System, 23(8), 1467-1479.
E. Liu, P., Wang, J., Ma, H., & Nie, H. (2014). Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE. Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 584-589). IEEE.
F. Adi Shamir.Identity-based cryptosystems and signature schemesIn Proceedings of CRYPTO 84 on Advances in cryptology, pages 47-53, Springer-Verlag New York, Inc, 1985.
G. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. (pp. 457-473). Springer.

H. Pandey, O., Goyal, V., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security, (pp. 89-98).
I. Zhang, B., & Zhang, F. (2011). An efficient public key encryption with conjunctive-subset keywords search. Journal of Network and Computer Applications, 1, 277-288.
J. Florence, M.L., Suresh, D. Enhanced secure sharing of PHR's in cloud using user usage based attribute based encryption and signature with keyword search. Cluster Comput 22, 13119–13130 (2019). https://doi.org/10.1007/s10586-017-1276-7.
K. Yinlai, J., Hayashi, I., & Wang, S. (2014). Knowledge Acquisition Method Based on Singular Value Decomposition for Human Motion Analysis. IEEE Transactions on Knowledge and Data Engineering, 26(12), 3038 3050.
L. Kamara, S., & Papamanthou, C. (2013). Parallel and dynamic searchable symmetric encryption. International Conference on Financial Cryptography and Data Security Proceeding (pp. 258-274). Financial Cryptography Data Security.
M. Karakoyunlu, D., Gurkaynak, F., Sunar, B., & Leblebici, Y. (2010). Efficient and side-channel-aware implementations of elliptic curve cryptosystems over prime fields. IET Information Security, 4(1), 30 - 43.
N. Suresh, D., Florence, M.L. Securing Personal Health Record System in Cloud Using User Usage Based Encryption. J Med Syst 43, 171 (2019). https://doi.org/10.1007/s10916-019-1301-x.