International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Scalable and Secure Sharing in Cloud Computing Using Data Manipulation & Encryption

Aakanksha Maliye[1], Sarita Patil[2]

[1]P. G. Student, Computer Department, GHRCEM, Pune, India.

[2]Professor, Computer Department, GHRCEM, Pune, India.

Abstract: ***Personal health record is using for maintaining the patient's personal and diagnoses information using one centralize server. Under the health information exchange server PHR is an emerging patient centric data model which is supposed to be outsources on the third party servers like cloud servers. The security scheme are mostly used for provide security of personal health record form public access at online. In this paper used encryption method is a promising method to assure patient's control over their own PHR's before outsourcing. Few such issues like privacy concern, scalability, flexibility and efficient user revocation are remained the most important challenges. To achieve secured and scalable data access control for PHRs, in this paper leverage attribute based encryption technique to encrypt each patient's PHR file. Different from existing system in secure data outsourcing , in this paper focus on the multiple data owner scenario in PHR system into multiple security domain that greatly reduce the key management complexity for owners & users. The paper is also enables user revocation on dynamic modification of access policies or file attribute.***

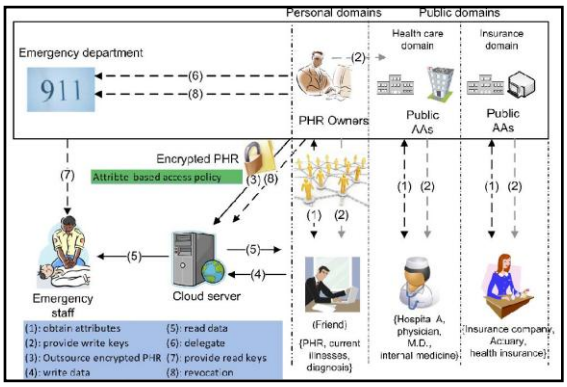
Keywords: Cloud computing, data privacy, personal health records, attribute-based encryption, file based encryption, attribute revocation

1. Introduction

In this cutting edge technology the cloud computing is one of the most emerging technologies where online services and application are provided via internet. At the cheapest cost on dynamic network to access multiple resources the cloud computing can be consider with greater flexibility and availability. Now a days the cloud computing is looking as a valuable partner to reduce cloud computing cost and to improve work productivity. The recent advancements in the cloud computing technology are to help large enterprises to reducing the computing costs while boosting work productivity. Growing enterprise interest in cloud on computing to rise Software as a Service (SaaS) based application. In the upcoming decades cloud servers and cloud technologies are going to become a pillar for world trade and most commonly used by end users.

Experienced by users of services which are usually offered by Apple Inc. Google Inc., Amazon Inc., or other services provider are clear indications that cloud is intrinsically insecure from a user's view point. Just because of the users can not access internal option of cloud services it is a great challenge for researchers. Cloud services are providing benefits to achieve versatile user of resources, specialization, and other scalable efficiencies.

Internet has been rapidly growing into a world of its own capabilities; Its huge space now offers various verities that support Physicians also in their duties in different and numerous ways. In the recent years, there is emerging trend and PHRs is model of health information exchange and management. A PHR is an online electronic record data of an individual's health information by which the individual controls access to their information and may have the ability to manage, track, and participate in their own health care. Generally, PHR service allows a user to control, create and manage their personal health record data in centralise place through the web, which has made storage, retrieval, and sharing of their personal medical information more efficient and secure. The general principles of the security rule include that covered entity must maintain "flexible, scalable, reasonable and appropriate" administrative techniques, and physical safeguards to protect Electronic Personal Health Information (e-PHI), it includes the requirements to ensure confidentiality, integrity, and availability of personal information.



2. Literature Survey

In this paper the mostly related work is about cryptographically access encrypted outsourced PHR files. To achieve fine-grained access control, the traditional public key (PKE) based scheme, either incur high key manage overhead, or require multiple level of file encryption using different keys. To improve the scalability of above solution one-to-many encryption method like ABE can be used. Encryption of data under the set of attributes can decrypt by multiple user who has proper keys.

2.1. Data Encryption Standard (DES):

Data Encryption Standard (DES) is a method which is using on wide range for data encryption with a secure and private key. To judge that key is so difficult to break by the U.S.

government because it was restricted for exportation to other countries. There are more than 72 quadrillion possible keys can be used. For each key message is chosen at random from among enormous number. Such as other private or public key cryptographic methods, it is necessary to use both the sender and the receiver the same private key.

2.2. ABE for Fine-grained Data Access Control:

Attribute-Based Encryption (ABE) is a generalized identity based encryption that incorporates attributes as inputs to its cryptographic primitives. Using a set of attribute the data will be encrypted so that multiple users with a proper process can decrypt the data. Attribute Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion.

2.3. Key Policy Attribute Based Encryption:

This is the modified method of the classical ABE model. The KP-ABE is a scheme which is associated with multiple key and data policies. The keys only associated with such policy that is to be satisfied by the attributes that are associating the data can decrypt the data. In this scheme public key encryption technique is designed for one-to-many communications which enables a data owner to reduce most of the computational overhead at cloud servers. The use of this encryption scheme KP-ABE provides fine-grained access control. While using the public domain, we can use multi authority ABE (MA-ABE) for improving the data security and avoid key escrow problem. In the data file each attribute authority (AA) is governs a dis-joints subset of user role attributes, while none of them are able to control the security of the whole system. We propose simple mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption.

3. Problem Statement

Under the problem statement the analysis of file based encryption before uploaded on private cloud server using DES algorithm of hybrid encryption with this cryptosystem. DES is most used throughout the world for protecting information. Data Encryption Standard (DES) is stronger than the other cryptosystems in this security because the process time required for crypto analysis has lessened, because of the hardware technique has developed rapidly, the DES may be attacked by various kinds of cryptanalysis using parallel process. It may be especially vulnerable to attack by differential cryptanalysis.

There has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). First its usually assume usage of a single trusted authority (TA) in the existing system. This is not only creating a load bottleneck, but also suffers from the lack of key escrow problem since the TA can access all the encrypted files for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys. In fact, different organizations usually form their own (sub) domain. For example, in a professional association would be responsible for certifying medical specialties, a regional health provider would certify the job ranks of its staffs.

4. Disadvantages

There is still lacks an efficient and on-demand user revocation mechanism for ABE & DES with the support for dynamic policy updates/changes, which is essential parts of secure PHR sharing. Finally most of the existing works do not differentiate between the personal and public domains (PUDs), which have different attribute definitions, key management requirements, and scalability issues.

5. Revocable DES

There is a well-known challenging problem to revoke attributes efficiently. In general tradition, this is often done by the provider broadcasting periodic key updates to unrevoked the users key frequently, does not achieve complete backward / forward security and is not sufficient. CP-ABE schemes are immediate attribute revocation capability, instead of periodical revocation. Even there is main advantage of its solution is, each user can be obtained some secret keys from any subset of the TAs in the system. The ABE scheme enjoys better policy expressiveness, and it is extended by to support user revocation. On the other downside, the communication of overhead key revocation is still not high, as it requires a data owner to transmit an updated cipher text component to every non revoked user. There is also can not differentiate personal and public domains.

6. Implementation

6.1. Attribute Based Encryption (ABE)

Process of PHR File Encryption
Step 1. Entering patient's personal data
Step 2. Entering patient's deices data
Step 3. Entering patient's insurance data
Step 4. Generate a unique file name
Step 5. Adding patient's data into file
Step 6. Generate a password for PHR file
Step 7. Encrypt file with password
Step 8.Save encrypted file on private cloud server.
Step 9. Exit

6.2. Process of PHR File Decryption:

Step 1. Entering patient's file name
Step 2. Entering file password (along with the PHR file)
Step 3. If entered details are correct, file has been decrypted
Step 4. File will open in decrypted format
Step 5. Exit

6.3. Hybrid Encryption

Process of PHR File Encryption Using Hybrid Encryption
Step 1. Entering patient's personal data
Step 2. Entering patient's deices data
Step 3. Entering patient's insurance data

Step 4. Encrypt patient's data
Step 5. Generate a unique PHR file
Step 6.Generate a random password for PHR file
Step7.Adding encrypted patient's data into file
Step 8. Adding random password to file
Step 9. Encrypt file with password
Step 10. Save encrypted file on private cloud server.
Step 11. Exit

6.4. Process of PHR File Decryption Using Hybrid Encryption

Step 1. Entering patient's file name
Step 2. Entering file password (One time password)
Step 3. If entered details are correct, file has been decrypted
Step 4. If file decrypted then PHR data will be decrypted
Step 5. File password will change for next time decryption
Step 6. File will open in decrypted format
Step 7. Exit

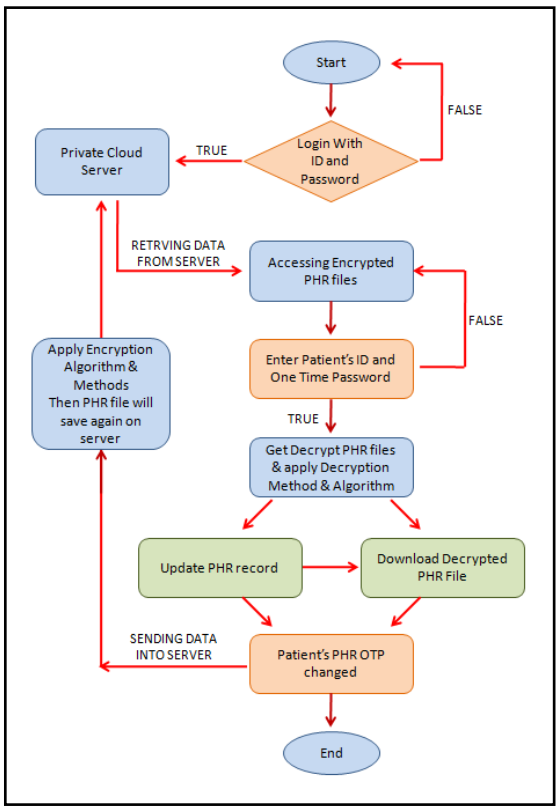


Figure 1: ER Diagram of implementation steps

7. Mathematical Module

Let p be a prime number, which is chosen randomly. The elliptic curve $Y2 = X3 + AX2 + B$ is chosen such that, A and B should satisfy the condition: $4A3 + 27B2 \neq 0$.This is to avoid duplication of roots. Since ECC is based on prime fields, curve equation and the conditions changes to equation 1 and 2 respectively.
$Y2 mod\ P = X3 + AX2 + B\ mod\ P$; $4A3 + 27B2\ mod\ P \neq 0$
By assigning a random value for X, corresponding value of Y can be found using the equation 3 in order to get the base point:
$Y = \pm\ \square\ (X3 + AX2 + B)\ mod\ P$; Let a = $X3 + AX2 + B$. Therefore, $Y = \pm\ \square\ a\ mod\ P$
Now `a' is a quadratic residue if $a\ P-1/2 \equiv 1\ (mod\ P)$.
Also, `a' is not a quadratic residue if $a\ P-1/2 \equiv -1\ (mod\ P)$.
Assuming that `a' is a quadratic residue, then $\square\ a\ mod\ P$ is calculated as shown below:
$P - 1 = 2\ .m$
z = any non residue mod p
$c \equiv zm\ (mod\ P)$
$u \equiv am\ mod\ P$
$v \equiv a\ m+1\ /\ 2\ (mod\ P)$
Note that o(c) is $2s$ and o(u) divides 2s-1 , as u is a quadratic residue. Also, $v2 \equiv ua\ (mod\ P)$. Each pass starts with o(u) dividing $2i$. Either o(u) divides $2i-1$, or $u2i-1 \equiv 1\ mod\ P$. In the latter case u and v can be modified as to make o(u) divide $2i-1$, while maintaining the property $v2 \equiv ua\ (mod\ P)$. Finally v is the square root of `a mod P' . Hence (X, Y) forms the base point G.
Now the order `n' of point G is found such that n(G)=O by performing scalar multiplication. Scalar multiplication requires two important operations namely point addition and point doubling [2].

A. Point Addition.
Let P(x1, y1) and Q(x2, y2) € (K) where P ≠ Q. Then P + Q = (x3, y3), where coordinates x3 and y3 are found using equation 4 and 5 respectively.
$x3 = (y2-y1\ /\ x2-x1\ )2 - x1 - x2$
$y3 = (y2-y1\ /\ x2-x1\ )2 - (x1 - x3) - y1$

B. Point Doubling.
Let P(x1, y1) € K(a,b) where P ≠ P then, 2P = (x3, y3); where coordinates x3 and y3 are found using equation 6 and 7 respectively.
$x3 = (\ 3x\ 2\ 1 + a\ /\ 2y1\ )2 - 2x1$
$y3 = (\ 3x21+a\ /\ 2y1\ )2 - (x1 - x3\ ) - y1$

C.Point Multiplication.
Let P be any point on the elliptic curve(K). Then the multiplication operation of the point P is defined as repeated addition, i.e. kP = P + P + ...k times. So, a random value k <n is chosen as ECC private key and perform scalar multiplication with base point in order to obtain the ECC Public Key PK, i.e. PK = k * G. Further, prime numbers p and q which are nearest to the coordinates of PK are obtained and are used to find jacobian symbols in Goldwasser Micali algorithm.

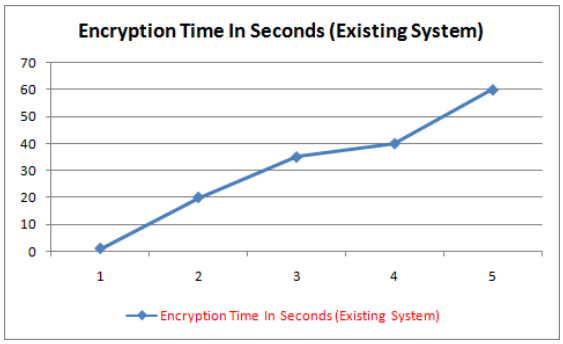
D. Integration.
The pair (p,q) acts as private key for Goldwasser Micali algorithm. Public key is constructed using N = p_q. Then, y is found such that Jacobian condition[12] is satisfied which is given as,
$y\ /\ N = 1$ ie $/\ p = y\ /\ q = 1$
where y is a pseudo square modulo Zn. Now (n,y) pair is the obtained public key.

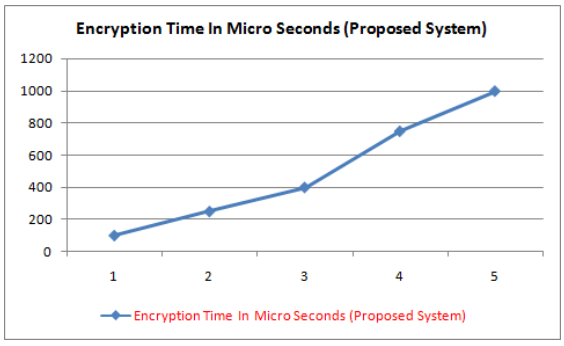
E. Encryption and Decryption
Let's assume that, sender A wants to send a message M to the receiver B. Through a standard key exchange mechanism, A obtains B's public Key i.e. (n, y). Message translator converts message M into a binary string as $m0,1,m2\ \ldots\ mi\ \ldots\ mn$. If ith bit of the message is mi, then using a pseudo random number x, corresponding cipher bit ci is computed as,

$ci = (y.x2 \ mod \ n) \ if \ mi = 1$
$ci = x2 \ mod \ n) \ if \ mi = 0$
So $c0,1,c2 \ldots \ldots \ldots . . ci \ldots \ldots . . cn$ is the generated string of cipher bits. While decrypting, receiver B obtains the cipher from A through communication channel. B uses its private key (p, q) to decipher the message. For each cipher bit , Legendre symbol is computed as:
$ei = ci / p$
If $ei = 1$, then set $mi = 0$ else set $mi = 1$. Finally, $m0m1m2 \ldots \ldots \ldots mi \ldots \ldots \ldots . mn$ is the decrypted message in the form of binary string. Message translator at receiver end converts this binary string into original message.

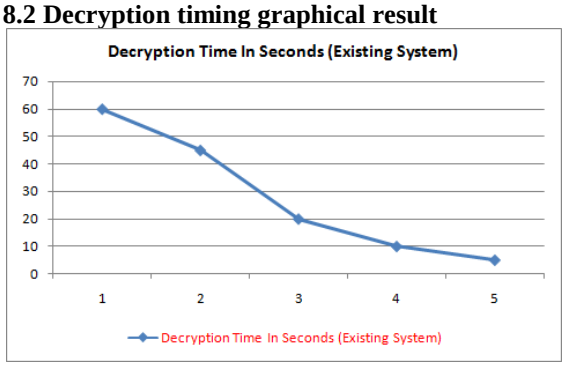
8. Graphical Result

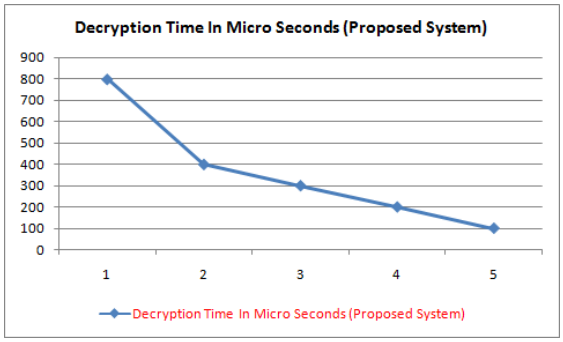
8.1 Encryption timing graphical result





8.2 Decryption timing graphical result





9. UML Diagram

Unified Modelling Language is a general purpose visual modelling language that is used to specify, visualize, construct and document the artefacts of the software system. It captures decision and understanding about the system that must be constructed. It is used to understand, design, browse, configure, maintain, and control information about such systems.

UML gives standard way to write systems blue prints covering conceptual thins, such as business processes and system functions, as well as concrete things, such as classes written in other programming languages, search schemas, and reusable software components.

Use Case Diagrams are useful for modelling the dynamic aspects of the systems. Use case diagrams are central to modelling the behaviour of the system, a subsystem or a class. They show a set of use cases and actors and their relationships.

Use Case Diagrams commonly contain the following:
1. Use cases.
2. Actors.
3. Dependency,generalization and associate relationships.

Use Case Diagrams are commonly used for:
1. To model the context of the system.
2. To model the requirements of the system

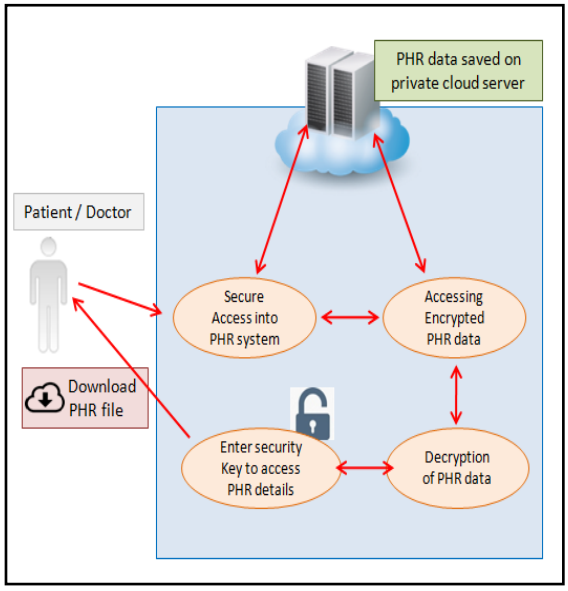


Figure 2: Use case Diagram

10. Future Enhancement

The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations.

11. Proposed System

Analysis of file encryption before uploaded on private cloud server using DES algorithm of hybrid encryption with this cryptosystem which is most used throughout the world for protecting information is the Data Encryption Standard (DES). The DES must be stronger than the other cryptosystems in its security because the process time required for cryptanalysis has lessened, and because hardware technique has developed rapidly, the DES may be attacked by various kinds of cryptanalysis using parallel process. It may be especially vulnerable to attack by differential cryptanalysis.

12. Aims and Objectives

In this project we have main aim is to provide secure searching:

- To present literature review different techniques used for semantic contents extraction.
- To present the design of proposed approach and algorithms.
- To present the practical analysis proposed algorithms and evaluate its performances.
- To present the comparative analysis of existing and proposed algorithms in order to claim the efficiency.

13. Scope

Our work presents a scalable way for the users to automatically form rich profiles. Such profiles summarize user's interests in an organization rendering to specific interests. In future we enhance an existing DES scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient. We can provide good security to our data's using encryption technique in cloud. In practice, the credentials from different organizations may be considered equally effective, in that case distributed DES schemes, will be needed.

References

[1] Securing the E-Health Cloud, H. Lohr (Proc. First ACM Int'l Health Informatics Symp. (IHI '10),pp. 220-229, 2010).
[2] Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records (Proc. ACM Workshop Cloud Computing Security(CCSW '09),pp. 103-114, 2009).
[3] Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data (Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006).
[4] Data Security and Privacy in Wireless Body Area Networks (IEEE Wireless Comm. Magazine, vol. 17,no. 1, pp. 51-58, Feb. 2010).
[5] Identity-Based Encryption with Efficient Revocation (Proc. 15th ACM Conf. Computer and Comm. Security (CCS),pp. 417-426, 2008).
[6] Improving Privacy and Security in Multi Authority Attribute Based Encryption (Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009).