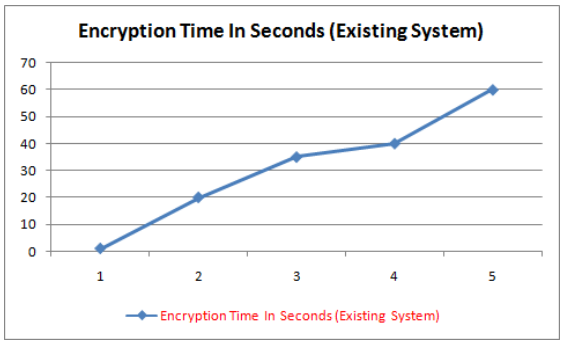
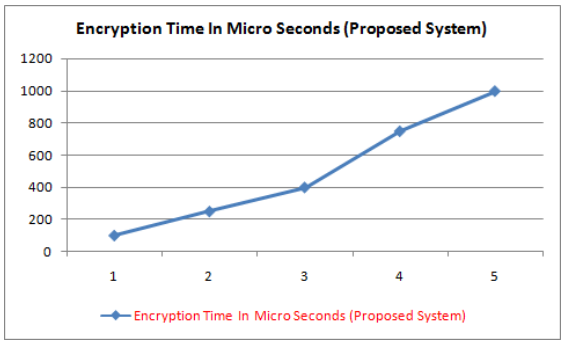
$ci = (y.x2 \ mod \ n) \ if \ mi = 1$
$ci = x2 \ mod \ n) \ if \ mi = 0$
So $c0,1,c2 \ldots \ldots \ldots . . ci \ldots \ldots . . cn$ is the generated string of cipher bits. While decrypting, receiver B obtains the cipher from A through communication channel. B uses its private key (p, q) to decipher 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.

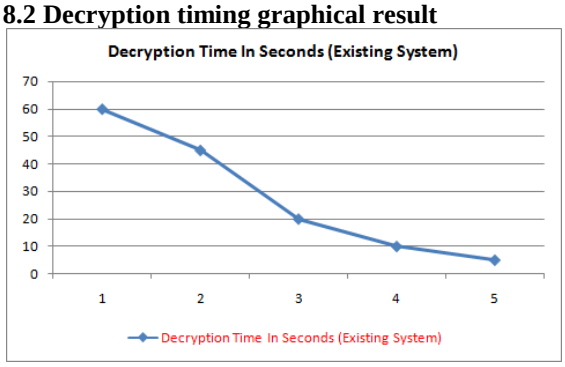
8. Graphical Result

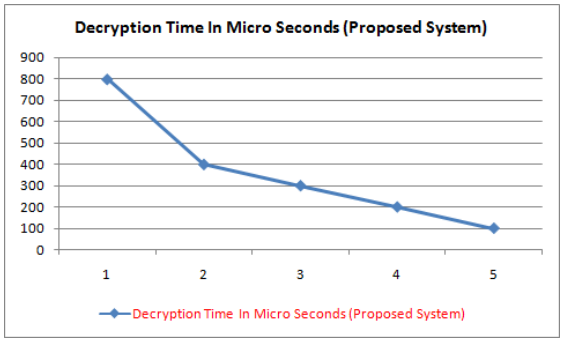
8.1 Encryption timing graphical result





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

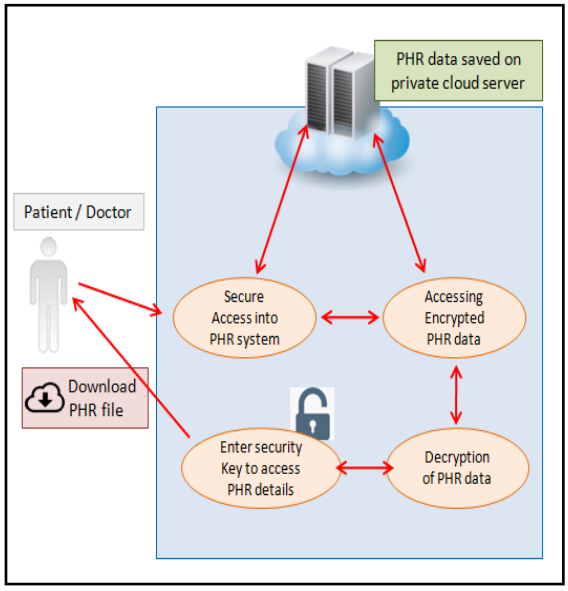


Figure 2: Use case Diagram

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).