Re-Encryption for Data in Transit and Data At Rest in Cloud Environment

Dr. R.Sumathi[1], S.Logaranjani[2], S.Swetha Sree[3], N.Poornima[4]
[1, 2, 3, 4] Department of Information Technology
[1, 2, 3, 4] Saranathan college of engineering, Trichy-620 002, Tamil Nadu.

Abstract- *In the recent developments of security in applications which require the information to be highly confidential, the purpose of encryption and re-encryption becomes an essential criterion. To enhance the security in cloud environment a number of Proxy Re-encryption techniques have been proposed namely Conditional Proxy Re-encryption (CPRE), Identity Based Proxy Re-encryption (IPRE) and Broadcast Proxy Re-encryption (BPRE). By incorporating the above techniques a versatile, primitive technique called Conditional Identity based Broad cast Proxy Re-encryption (CIBPRE) that formalizes semantic security is referred.*

CIBPRE works by specifying the receivers' identity in order to allow the sender to encrypt a message to the intended multiple receivers. The conversion of cipher-text into a new format of Re-encrypted message for a new set of receivers can be achieved by the sender by delegation of a re encryption key to a proxy. This approach provides an efficient and provable security. The Re-encrypted cipher text, initial cipher text and the Re-encryption key are all in constant size and the receivers' initial cipher text does not depend on the Re-encryption key.

Keywords- Encryption, Re-encryption, Proxy, CPRE, IPRE, BPRE, CIBPRE, Cipher text, Encryption key.

I. INTRODUCTION

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources which can be rapidly provisioned and released with minimal management effort.

Proxy re-encryption schemes are cryptosystems which allow third parties (proxy) to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. The early PRE was proposed in the traditional public key infrastructure setting which incurs complicated certificate management. To relieve from this problem, several IPRE schemes were proposed so that the receivers' recognizable identities can serve as public keys. Instead of fetching and verifying the receivers' certificates, the sender and the proxy just need to know the receivers' identities, which is more convenient in practice.

II. NET FRAMEWORK

.NET is a "Software Platform". It is a language-neutral environment for developing rich .NET experiences and building applications that can easily and securely operate within it. When developed applications are deployed, those applications will target .NET and will execute wherever .NET is implemented instead of targeting a particular Hardware/OS combination. The components that make up the .NET platform are collectively called the .NET Framework. The .NET Framework is a managed, type-safe environment for developing and executing applications. The .NET Framework manages all aspects of program execution, like, allocation of memory for the storage of data and instructions, granting and denying permissions to the application, managing execution of the application and reallocation of memory for resources that are not needed. The .NET Framework is designed for cross-language compatibility.

The .NET Framework consists of two main components:

- Common Language Runtime (CLR)
- Class Libraries

Advantage of C#.NET:

i. C# borrows concepts from Java and C++, adopting only the good bits from those languages and eliminating overly confusing and error prone features, which are the major sources of bugs in a code. C# is a terse language. It's very tiny even with the commands. Visual Basic on the other hand has a command for almost any kind of situation that the developer may face during the development of the code making its reference a real hefty one. C# supports effective and reusable components.

ii. C# programs can be written in as simple as a textpad and a command line which are common to any

operating system provided the developer has installed the CLR and the framework priorly. Microsoft's Rapid Application Development Suite products, named Microsoft Visual Studio ships with a separate Visual tool for C#, and gives developers visually rich tools for development and deployment.

iii. C# RAD tools gives the developer the power to produce "One click install" application, where the user needs no prior software experience and can install and use C# applications like any other windows program.

iv. C# provides the ability of code extension to the developer with which developers can produce extensions and wrappers to use the underlying library to behave the way the developer want it to.

v. C# programs are managed code, to say, they are coded and executed in a controlled environment leaving little room for anamolies called "bugs" to creep in. Also it has eliminated some of the "unsafe" features of C++, which can provide intruders to breach secure C# programs.

vi. Due to their high portability, they are used for web programming and with new information sharing concepts like web services, they bring distributed information sharing to the very desktop of the user and all that the user needs is a computer and a browser.

vii. C# hides low level details from the application developer and provides with a wide range of library functions which a developer can utilize to produce code for almost any kind of application and focus on the logic of the application and need not bother about its compatibility with other windows machines.

viii. C# can be used to write wide range of applications due to their portability, from simple desktop widgets to high end web services, secure systems programming and even robotics.

ASP.NET is more than the next version of Active Server Pages (ASP); it is a unified Web development platform that provides the services necessary for developers to build enterprise-class Web applications. While ASP.NET is largely syntax compatible with ASP, it also provides a new programming model and infrastructure for more secure, scalable, and stable applications. You can feel free to augment your existing ASP applications by incrementally adding ASP.NET functionality to them.

III. OBJECTIVE

The main objective is to refine PRE by incorporating the advantages of IPRE, CPRE and BPRE for more flexible applications and propose a new concept of conditional identity based broadcast PRE (CIBPRE). In a CIBPRE system, a trusted key generation center (KGC) initializes the system parameters of CIBPRE, and generates private keys for users. To securely share files to multiple receivers, a sender can encrypt the files with the receivers' identities and file-sharing conditions. If later the sender would also like to share some files associated with the same condition with other receivers, the sender can delegate a re-encryption key labeled with the condition to the proxy, and the parameters to generate the re-encryption key is independent of the original receivers of these files. Then the proxy can re-encrypt the initial cipher texts matching the condition to the resulting receiver set. With CIBPRE, in addition to the initial authorized receivers who can access the file by decrypting the initial cipher text with their private keys, the newly authorized receivers can also access the file by decrypting the re-encrypted cipher text with their private keys. Note that the initial cipher texts may be stored remotely while keeping secret. The sender does not need to download and re-encrypt repetitively, but delegates a single key matching condition to the proxy. These features make CIBPRE a versatile tool to secure remotely stored files, especially when there are different receivers to share the files as time passes.

Advantages:

1. It allows a user to share their outsourced encrypted data with others in a fine-grained manner. All CIBPRE users take their identities as public keys to encrypt data.
2. It avoids a user to fetch and verify other users' certificates before encrypting his data.
3. Moreover, it allows a user to generate a broadcast cipher text for multiple receivers and share his outsourced encrypted data to multiple receivers in a batch manner.

IV. PROPOSED SYSTEM

This system is aimed at developing in a PRE system, a trusted key generation center (KGC) initializes the system parameters of PRE, and generates private keys for users to securely share files to multiple receivers.

Architecture:

Sender:

The sender has to register the details for accessing their account. After doing so, he/she has to login to the system.

Encryption:

The encryption process should take place when the sender combines their plain text with the public key (Provided the public key should be given by the KGC-Key Generation Centre) .This forms the first level of encryption.

Re-Encryption:

The Re-Encryption process takes place with the cipher –text and a combination of secret key and public key.

Proxy:

a proxy is a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different source .In this case the proxy does the Re-Encryption process.

Cloud Server:

A cloud server is a logical server that is built, hosted and delivered through a cloud computing platform over the Internet. Cloud servers possess and exhibit similar capabilities and functionality to a typical server but are accessed remotely from a cloud service provider. In the implementation perspective MySQL is used for similar functionality. MySQL is an open source relational database management system (RDBMS) based on Structured Query Language (SQL).

KGC:

In cryptography, a Key Generation Center (KGC) is part of a cryptosystem intended to reduce the risks inherent in exchanging keys. KGCs often operate in systems within which some users may have permission to use certain services at some times and not at others. A typical operation with a KGC involves a request from a user to use some service. The KGC will use cryptographic techniques to authenticate requesting users as themselves. It will also check whether an individual user has the right to access the service requested. If the authenticated user meets all prescribed conditions, the KGC can issue a ticket permitting access.

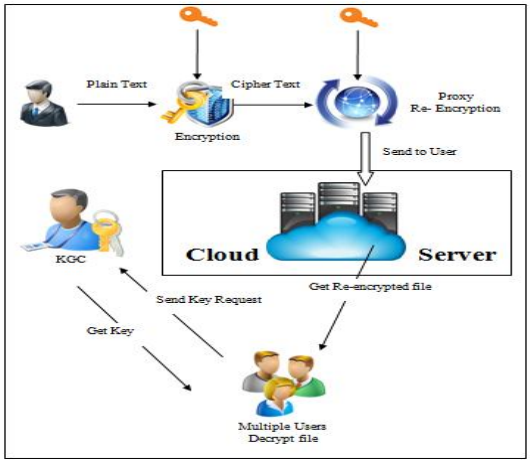

Figure 1.

ROLE OF KGC IN GENERATING PUBLIC KEYS:

This information is mainly about the involvement of KGC in generating keys for the sender and proxy respectively. The sender will do the first level of encryption by using the public key provided by the KGC. The KGC will also provide the session key and public key to the proxy so that the proxy can proceed with the Re-Encryption process by obtaining the cipher text from the previous step.

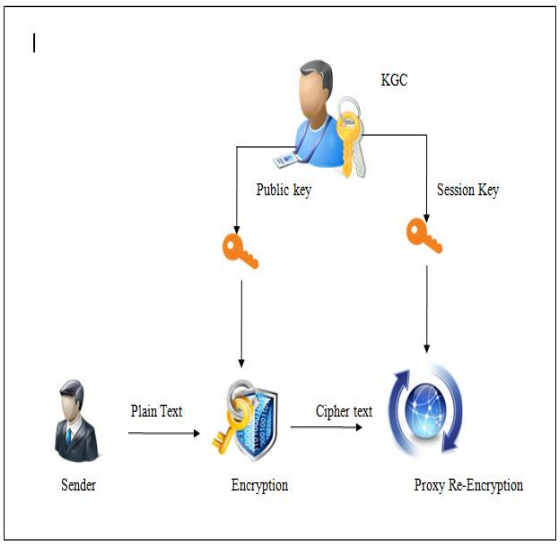

Figure 2.

It includes four modules mainly:

1. Data owner Encrypt File
2. Proxy Re-Encrypt File
3. Key Distribution Center
4. User Decrypt and Re-decrypt File

i. Data Owner Encrypt File

Data owner first Browse the text file. Convert the file as an encrypted format. Send file as an encrypted format to Proxy.

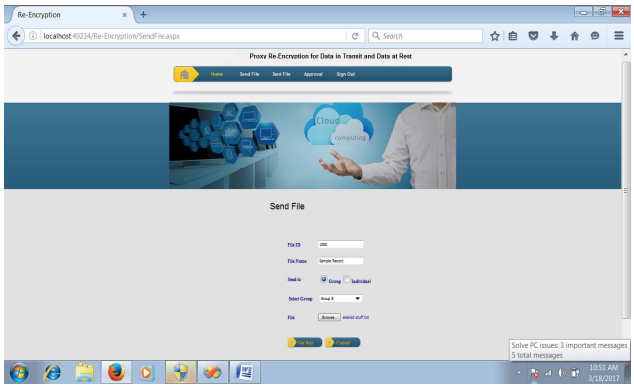

Figure 3.

ii. Proxy Re-encrypt File

Proxy Re-encrypt the cipher text received from the sender. It sends the re-encrypted file to the receivers

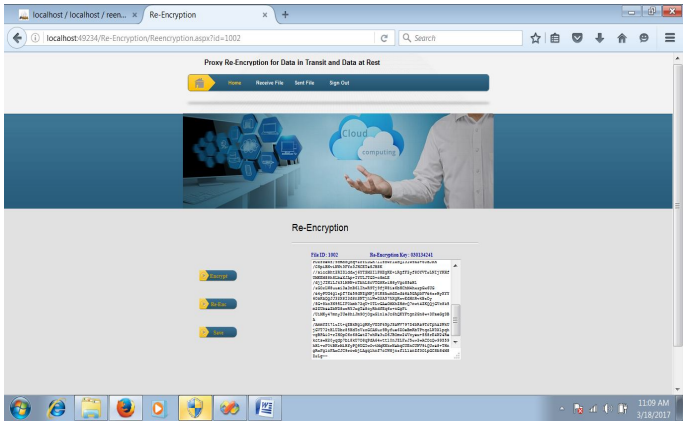

Figure 4.

iii. Key Distribution Center

User send request to the KGC(key generation center) for the key to decrypt the received file. The KGC sends the response as the key to the user.

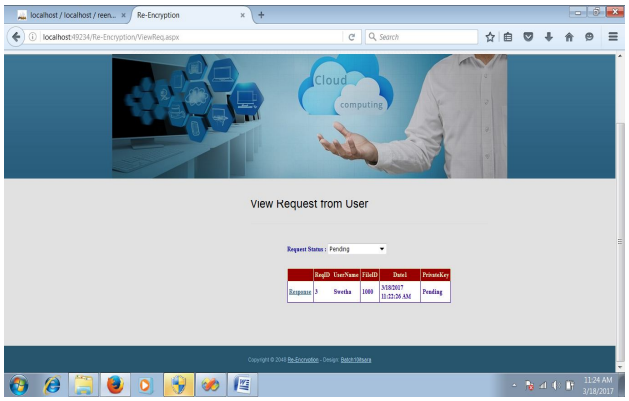

Figure 5.

iv. User Decrypt And Re-decrypt File

With the help of key from the KGC, users decrypt the received file. The decrypted file is decrypt again to get the original file.

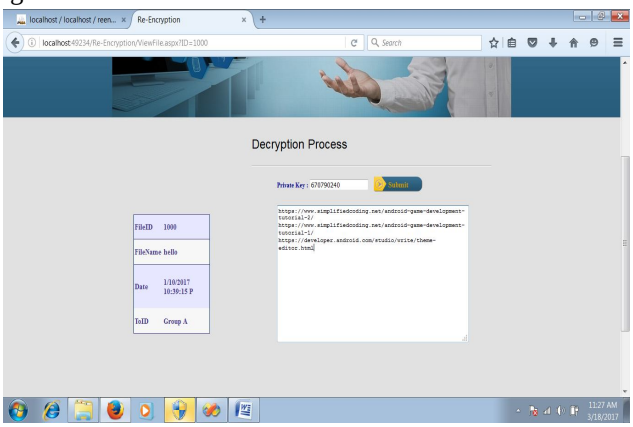

Figure 6.

V. CONCLUSION

The CIBPRE is a general concept equipped with the capabilities of conditional PRE, Identity-based PRE and broadcast PRE. It allows a user to share their outsourced encrypted data with others in a fine-grained manner. All CIBPRE users takes their identities as public keys to encrypt data. It avoids a user to fetch and verify other users' certificates before encrypting his data. Moreover, it allows a user to generate a broadcast cipher text for multiple receivers and share his outsourced encrypted data to multiple receivers in a batch manner. We instantiated the first CIBPRE scheme based on the Identity-based broadcast encryption in. Upon the provable security of the IBPRE scheme and the DBDH assumption, it indicates that without the corresponding private key or the right to share a user's outsourced data, one can learn nothing about the user's data. Finally, we compared the proposed CIBPRE scheme with similar works and the comparison confirms the advantages of our CIBPRE scheme.

We built the encrypted cloud email system based our CIBPRE scheme.

REFERENCES

[1] Jian Weng, Robert H. Deng, Xuhua Ding, Cheng-Kang Chu, Junzuo Lai, "CONDITIONAL PROXY RE-ENCRYPTION SECURE AGAINST CHOSEN-CIPHERTEXT ATTACK".

[2] R. Sumathi, Member, IACSIT and E.Kirubakaran, "SCEHSS: SECURED CLOUD BASED ELECTRONIC HEALTH RECORD STORAGE SYSTEM WITH RE-ENCRYPTION AT CLOUD SERVICE PROVIDER", Internatinal journal ofcomputer and communication engineering, Vol.2, No.2, March 2013.

[3] Kaitai Liang, Qiong Huang, Roman Schlegel, Duncan S.Wong, and Chunming Tang,"A CONDITIONAL PROXY BROADCAST RE-ENCRYPTION SCHEME SUPPORTING TIMED-RELEASE"

[4] Jian Weng, Yanjiang Yang, Qiang Tang, Robert H. Deng, and Feng Bao, "EFFICIENT CONDITIONAL PROXY RE-ENCRYPTION WITH CHOSEN-CIPHERTEXT SECURITY"

[5] Matthew Green, Giuseppe Ateniese,"IDENTITY-BASED PROXY RE-ENCRYPTION".