

An Efficient and Light weight Secure Framework for Applications of Cloud Environment using Identity Encryption Method

E.Sathiyamoorthy¹, S.S.Manivannan²

^{1&2} School of Information Technology and Engineering
VIT University, Tamil Nadu , India

¹esathiyamoorthy@vit.ac.in, ²manivannan.ss@vit.ac.in

Abstract :

Security plays a vital role in Cloud Computing Services. Public Key Encryption is the mostly used method to provide security that needs sharing the public keys and digital certificates. Securing the data and resources in the Cloud is a difficult task. If the security method adopted in cloud environment is not understandable by the user, then the user may leave the service or application. So an easy-to-use security method is required for cloud applications. In this paper we propose the light weight Secure Framework for Applications of Cloud Environment using Identity Based Cryptography that overcomes the problems of existing security approaches. A mail application is developed to demonstrate the simplicity of proposed approach using Identity-Based Cryptography. Our approach allows several domains to execute independently and clearly depicts the complexity involved in Certificate Based Infrastructures and encourages the use of novel Identity-Based Infrastructure ,which is easy to perform and less complex than the traditional public key algorithms.

Keywords :

Cloud Computing, Services, Security, Identity Based Cryptography, Less Complexity, Easy to use

1. Introduction

Cloud environment gives the best way to share services , resources and data. But providing the security in clouds is a challenging issue. Many service providers provide Cloud Computing Security. The commonly used security feature is public key encryption that requires pre-sharing of the public keys and digital certificates. It is difficult to understand how to protect the data and resources in the Cloud from a security breach. Thus a security approach must be identified that is comprehensible and easy-to-use Identity-based Security Infrastructure is proposed. The difficulty of using the PKI is managing the certificates and keys.

In asymmetric algorithm, public information is used to generate the public keys. So a client can generate the public key of others. The parameters such as client identity, client's position and key validity time are considered to generate the pair of keys. In public key cryptography, certificate authority verifies the certificate information. In identity based encryption, the trusted authority generates and distributes the key pairs.

Similar to network-based application, Cloud computing also have certain vulnerabilities in storage and communication. Providing physical access to the unknown third parties present in the network. In this paper, we have proposed the Identity Encryption method. The features of the proposed system are

- i) There is no need for any public key certificate.
- ii) It provides a very secure way of storing and retrieving data in the Cloud.
- iii) Operating Costs were one-fifth of those of Public key systems.
- iv) It requires a simpler infrastructure.

Thus it is more feasible to implement this security infrastructure in Cloud Environment.

2. Literature Survey

After doing a good study , it is clear that only limited number of attempts have been made to apply Identity-Based Cryptography to cloud computing . Identity based encryption proposed by Shamir [1] , solves the problem of authenticity of keys.

Asish Kuamr has proposed the cloud computing and security [2]. Cloud Computing provides the services such as virtualization and on demand deployment. An efficient security scheme is required to ensure the integrity of data in the cloud environments. A perfect cloud data security and performance is required to ensure the quality of services.

The practical and secure Identity-based Public Key Encryption Scheme was presented by Boneh and Franklin [3]. They proposed that the key escrow can be circumvented by using Multiple Trusted Authorities.

Sai Krishna Parsha and Mohd Khaja Pasha have proposed Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption [4]. They have proposed the deployment of data access security in cloud environments. Data access is restricted to un trusted users by organizing the users in a hierarchical method and the security is achieved by allowing only the trusted users to access the data.

Schridde and Christian have proposed the identity-based security infrastructure for Cloud environments [5]. An identity-based cryptographic approach that does not require a trust hierarchy is proposed. Traditional cryptography methods and identity-based cryptography methods are compared towards data transfer rate is presented.

Hongbing, Chunming, Zhenghua and Qingkai have proposed Identity Based Encryption and Biometric Authentication Scheme for Secure Data Access in Cloud Computing [6]. They proposed an integrated data access approach for cloud computing that uses parameter setup, key distribution, feature template creation, cloud data processing to provide the secure data access control.

Hongwei Li, Yuanshun Dai and Bo Yang have proposed Identity-Based Cryptography for Cloud Security [7]. They presented a Hierarchical Architecture for Cloud Computing (HACC) that uses Identity-Based Encryption (IBE) and Identity-Based Signature (IBS). Authentication Protocol for Cloud Computing (APCC) is presented to achieve high performance.

Lim and Robshaw [8] propose a Dynamic Key Infrastructure for Grids based on Identity-Based Encryption. In the same way, Lim and Patterson [9] suggest the use of identity-Based Cryptography as an alternative for GSI. Gentry and Silverberg proposed HIBC in [10] to ease the Private key Distribution problem and improve Scalability of the original IBE scheme.

Cramptom, Lim and Patterson examined how Identity-Based Cryptography can be used to secure Web Services [11].

Lim and Robshaw have presented the use of IBC in a Grid Security Architecture. They stated that the properties of IBC allows the generation of keys that is used as an alternative approach to provide good security [12].

3. Architecture

3.1. Architecture of the Proposed system:

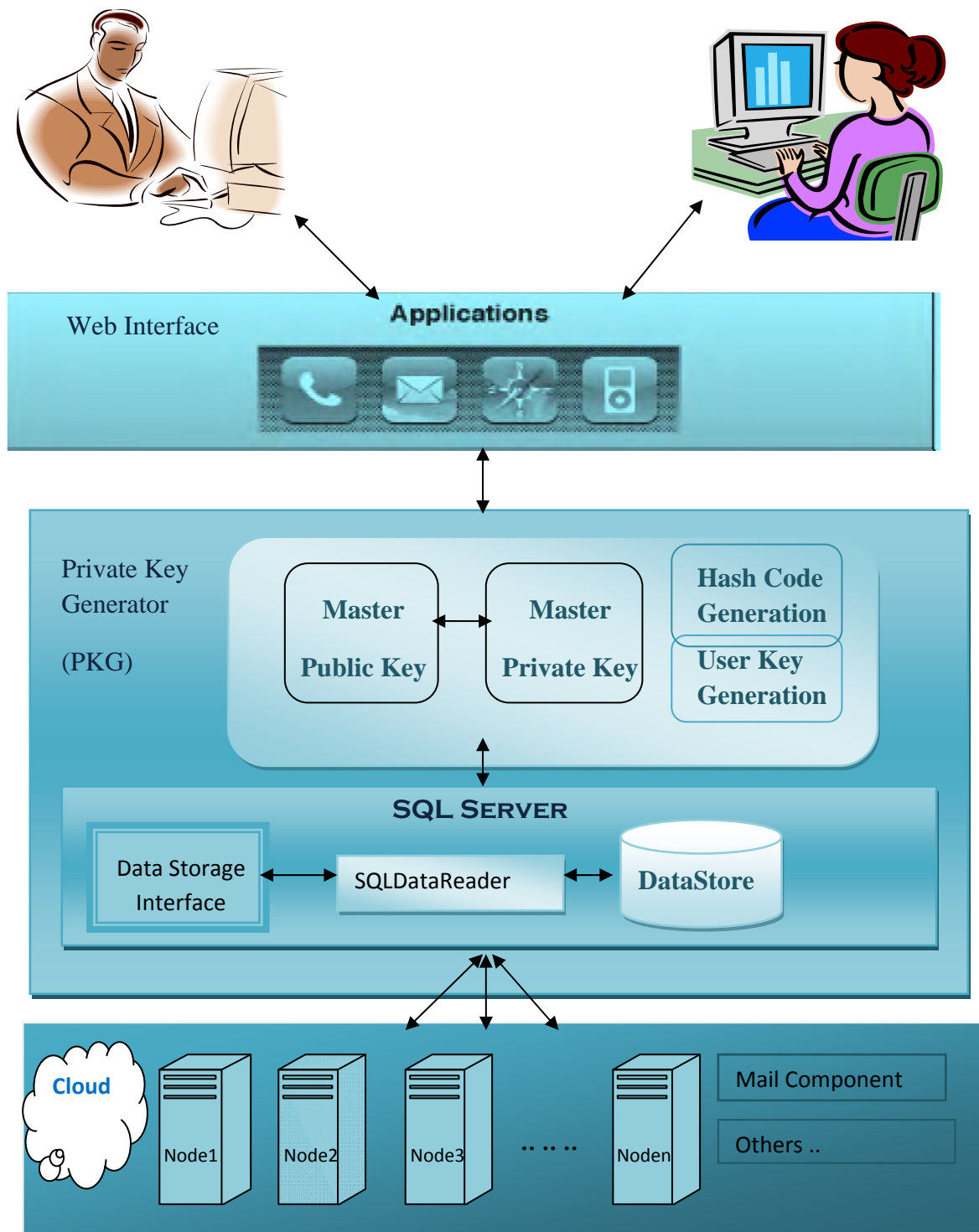


Fig.1 Architecture of Identity Based Cryptography

Web Interface layer acts as a mediator between the user and database and also between the user and the Third Party Server. This displays how the Identity based encryption secures the data that is stored in the cloud. Private key Generator acts as a middle layer between the Cloud and the user. This is also called as Trusted Authority (TA), since the user must trust this generator for secure transactions.

3.2 Components of Identity Based Encryption

The components of Identity Based Encryption is shown in the Fig.2

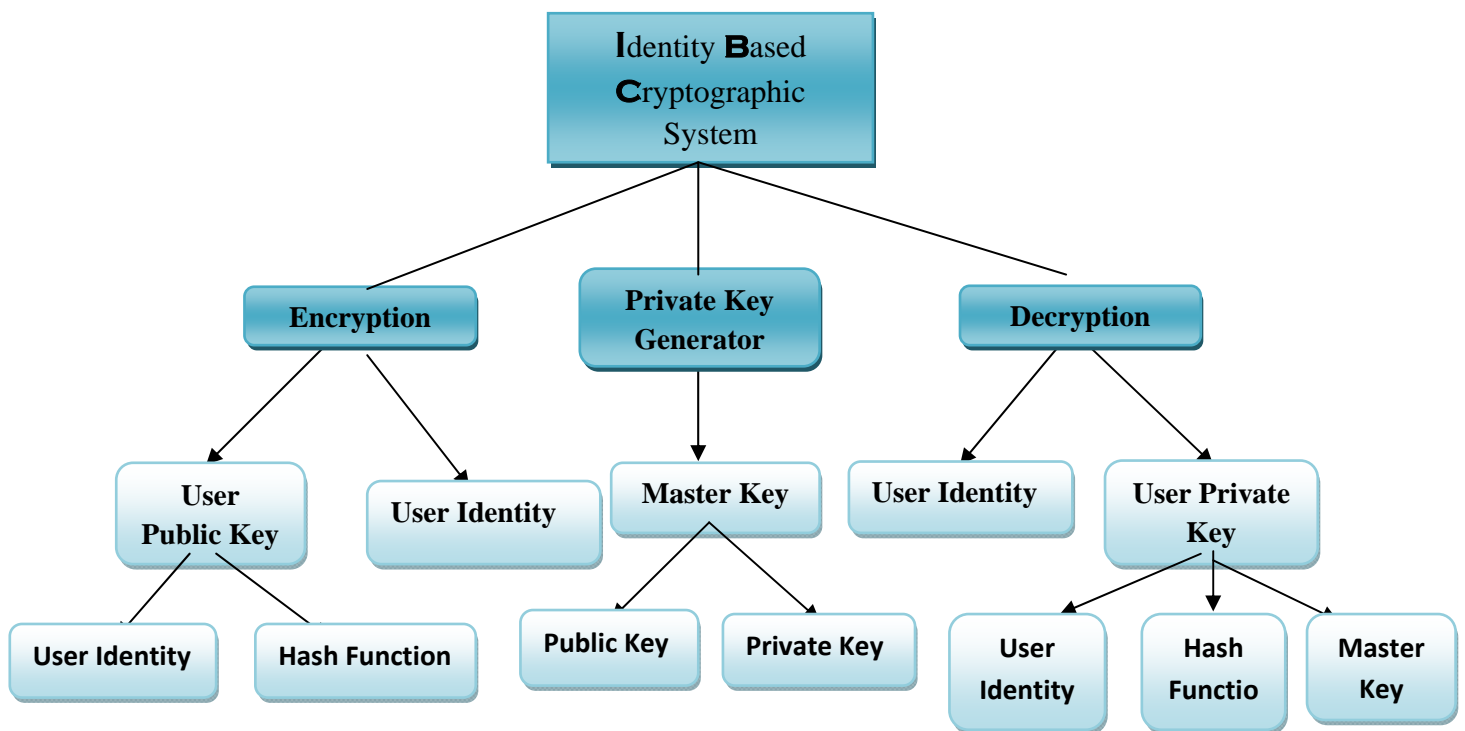


Fig.2 Components Identity-Based Cryptography

3.3 Design of a secure mail application using Identity based cryptography

Algorithm:

- i) Record the User information.
- ii) Create new Identity.
- iii) Record Identity details.
- iv) Encrypt the Message.
- v) Send to the Intended user.
- vi) Check Identity Availability.
- vii) Receive the cipher text mail.
- viii) Decrypt the message.

The following Fig.3 shows the detailed steps in encryption and decryption process.

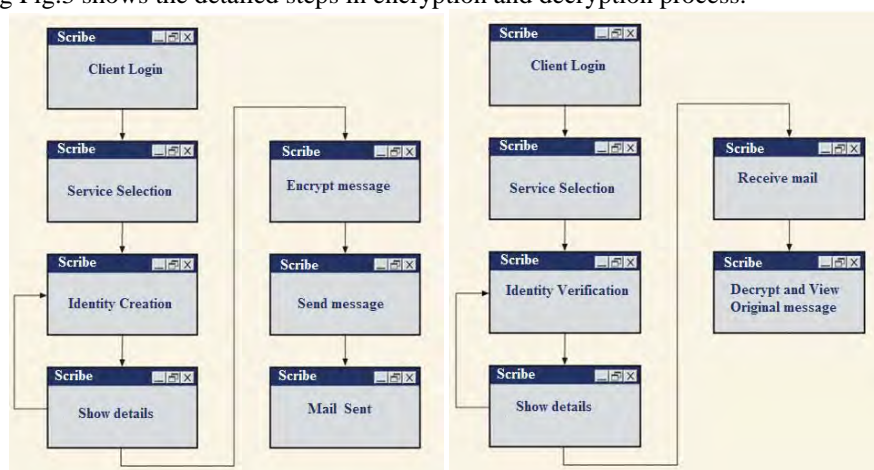


Fig.3 Encryption and Decryption Process

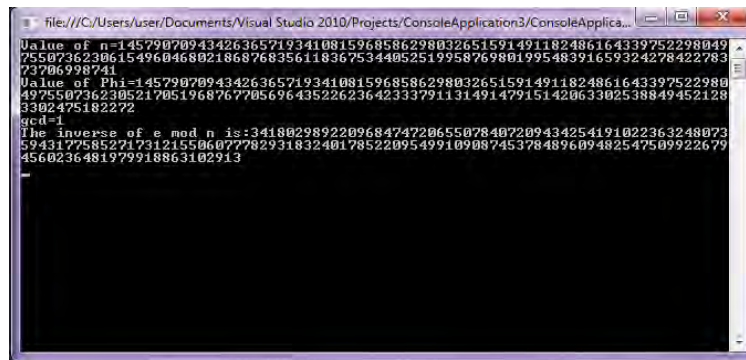
4. Implementation of Identity Based Cryptography

4.1 Generation of Public Shared parameters (PSP)

Algorithm : Extended Euclidean Algorithm is used to find the inverse of $e \bmod n$.

Input : Two large prime numbers[p,q].

Output : Public Shared Parameters



```

file:///C:/Users/user/Documents/Visual Studio 2010/Projects/ConsoleApplication3/ConsoleApplica...
Value of n=145790709434263657193410815968586298032651591491182486164339752298049
75507362306154960468021868768356118367534405251995076980199548391659324278422783
73706998741
Value of Phi=1457907094342636571934108159685862980326515914911824861643397522980
4975507362306154960468021868768356118367534405251995076980199548391659324278422783
3302475182272
gcd=1
The inverse of e mod n is:341802989220968474720655078407209434254191022363248073
59431775852717312155060777829318324017852209549910908745378489609482547509922679
4560236481979918863102913
  
```

Fig.4 Generation of Public Shared Parameters

4.2 Generation of Public Key Generation

Algorithm : Generation of Public Key

Input : Identity and hash algorithm type.

Output : Hash Value of Identity/User Public Key.

Public key is generated using only the user's identity by creating a hash value using SHA 256 or SHA 512 algorithm

4.3 Encryption Process

Description :To encrypt the message using the User Public Key.

Input : Message

Output : Encrypted text/Cipher text.

The formula used for encryption process

$$C = \text{message}^{H(id)} \bmod n, \text{ where } H(id) \text{ is the Hash Value of Identity.}$$

Fast Modular Exponentiation algorithm is used to do modular exponentiation

Fast Modular Exponentiation algorithm is extremely efficient and is very useful in our work relating to public key and elliptic curve cryptography:

Input : An integer base c, an integer exponent x and an integer modulus $m > 1$.

Output : A nonnegative integer a, m that satisfies $a = c^x \pmod{m}$.

Step 1 : Use Algorithm 1 to create the binary expansion of the exponent x :

$$x \sim [d_k d_{k-1} \dots d_1 d_0]_{(base\ 2)}$$

Step 2 : Repeatedly square the number $c \pmod{m}$ as we run through the binary digits d_k of x, including the result in the cumulative product only when $d_k = 1$.

Set $a = 1$ <Initialize cumulative product a>

Set $s = c \pmod{m}$ <Initialize squaring>

FOR $k = 0$ TO K

IF $d_k = 1$

Update $a \rightarrow a * s \pmod{m}$

END <IF>

Update $s \rightarrow s^2 \pmod{m}$ < Squaring need not be done when $k=K$ >
 END < k FOR >

Step 3 : Output : a

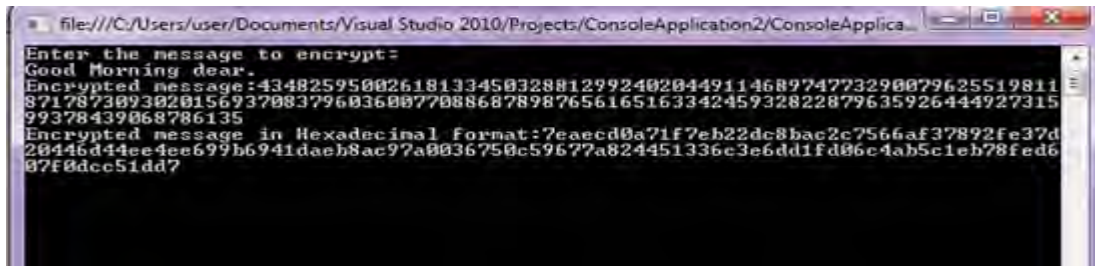


Fig.5 Encryption

4.4 User Private Key Generation.

Description : To generate User Private Key using PSPs.

Input : PSPs and Hash value of Identity .

Output : User Private Key.

User Private Key, $d = [H(id)^{-1} \pmod{\phi}] \pmod{n}$,

where n and phi are the Publicly Shared Parameters.

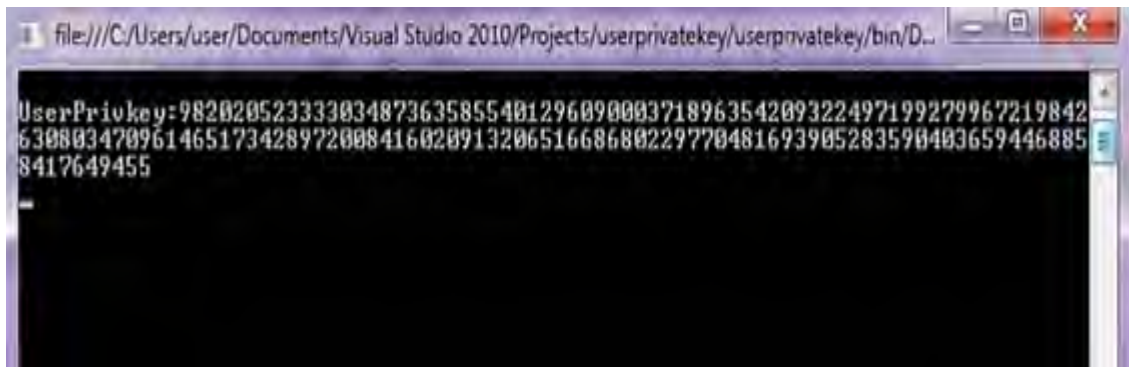


Fig.6 User Private Key Generation

4.5 Decryption

Description : To decrypt the message using the User Public Key.

Input : Ciphertext and User Private Key .

Output : Original message.

Decrypt , $M = \text{Ciphertext}^d \pmod{n}$, where d is the User Private Key.

The same Fast modular Exponentiation algorithm is used.

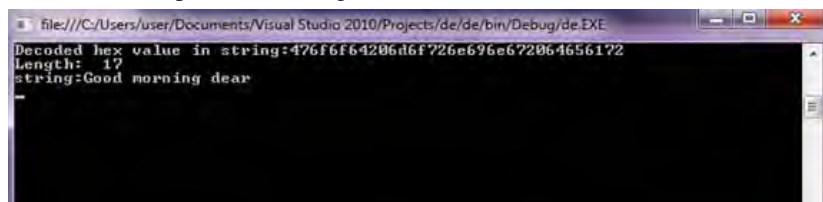


Fig.7 Decryption

5. Design of secure mail application using identity based encryption

To demonstrate the proposed system a e mail application SCRIBE (SeCuring Resources using Identity-Based Encryption) is developed using the identity based encryption.

5.1 Identity Creation Page :

The user can create a new Identity or use existing Identity by choosing one item. The identity will be immediately PostBack to the server for checking its Availability as shown below:



Fig.8 Identity Creation

Here the user selects “Create New Identity” and enters some existing identity, so a message is displayed that it already exists.

5.2 Use Existing Identity

If the user chooses “ Use Existing identity” and gives a new identity,it should immediately postback to the server and check the availability and display a message if it doesn’t exists :



Fig.9 Use Existing Identity

5.3 Using Calendar as the validity of Identity



Fig.10 Selecting Validity date for the Identity

5.4 Sending mail

Once Encryption is done, the interface will ask the user to provide the receiver’s email id to send the message .

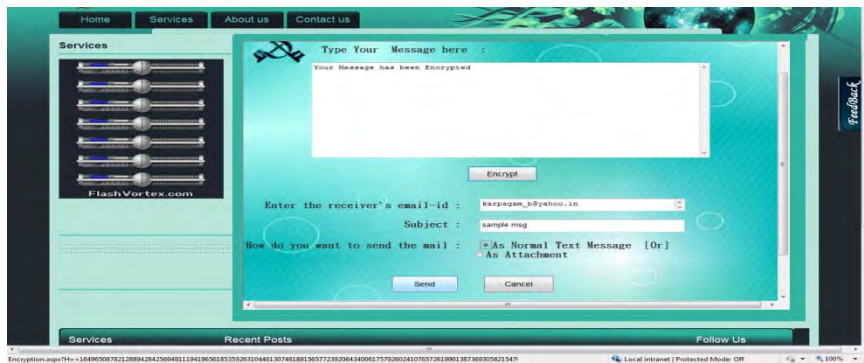


Fig.11 Sending the mail using encryption

5.5 Decrypt the content of email

After receiving the encrypted message ,decryption is applied to convert the cipher text back to original message.

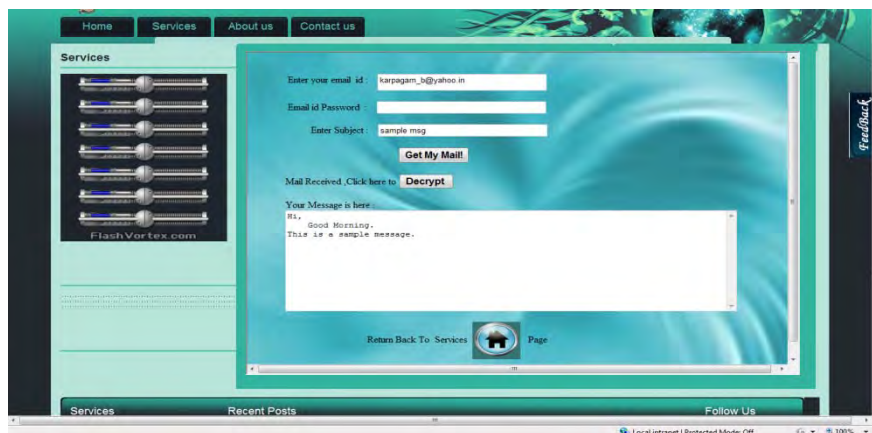


Fig.12 Decrypting the content of mail

6. Conclusion

In this paper, an efficient and light-weight Security frame work for Applications of Cloud Environment using Identity Encryption method was discussed which overcomes the problems faced by Certificate-based security. A mail application is developed to demonstrate the simplicity of proposed approach using Identity Based Cryptography. This approach indicates that an alternative secure framework can be developed for the applications of cloud environment that offers easy to use infrastructure rather than certificate based cryptography.

7. References

- [1] Adi Shamir, "Identity Based Cryptosystems and Signature Schemes", Advances in Cryptology, Lecture Notes in Computer Science, Vol:196, pp: 47-53, Springer,1984.
- [2] Ashish Kumar, "World of Cloud computing and Security", International Journal of Cloud Computing and Services Science, Vol.1, No.2, pp. 53-58, 2012
- [3] D.Boneh and M.Franklin. "Identity Based Encryption", Advances in Cryptology,Lecture Notes in Computer Science, pp:213-229, Springer-Verlag ,2001
- [4] Sai Krishna Parsha, Mohd Khaja Pasha, "Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption (HIBE)", International Journal of Scientific & Engineering Research, Vol: 3, No.5, pp:1-5, 2012
- [5] Christian, Bernd Freisleben, M.Smith, "An Identity-Based Security Infrastructure for Cloud Environments", IEEE International Conference on Wireless Communications Networking and Information Security, pp: 644-649,China, 2010.
- [6] Hongbing, Chunming, Zhenghua and Qingkai, "Identity Based Encryption and Biometric Authentication Scheme for Secure Data Access in Cloud Computing", Chinese Journal of Electronics Vol.21, No.2, 2012
- [7] Hongwei Li, Yuanshun Dai and Bo Yang, "Identity-Based Cryptography for Cloud Security", IEEE International Conference 2010
- [8] H.W.Lim and M.J.B. Robshaw, "A Dynamic Key Infrastructure for Grid", European Grid Conference on Advances in Grid Computing, pp:255-264,2005
- [9] H.W.Lim and K.G.Paterson, "Identity-Based Cryptography for Grid Security", Proceedings of the First international Conference on e-science and Grid Computing, pp: 395-404,IEEE press,2005.
- [10] C.Gentry and A.Silverberg, "Hierarchical ID-Based Cryptography",Advances in Cryptology, Lecture Notes in Computer Science,pp:48-566,Springer-Verlag, 2002
- [11] Crampton, H.W.Lim and K.G.Paterson, "What can identity Based Cryptography offer to Web Services ?", Proceedings of ACM Workshop on Secure Web Services, pages 26-36,ACM,2007
- [12] H.W.Lim and M.J.B. Robshaw. "On Identity-Based Cryptography and Grid Computing , ICCS ,pp.474-477,Springer-Verlag,2004