ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
ICRITCSA
M S Ramaiah Institute of Technology, Bangalore
Vol. 5, Special Issue 2, October 2016

Security Enhancement on Cloud using Identity Based Encryption (IBE)

Shruthi N [1], Kumar P K[2], Swamy L N[3] , Sukruth Gowda M A[4]

VI SEM Student, MCA, VTU, PG Studies, Muddenhalli, Bangalore, India [1]

Assistant Professor, MCA, VTU, PG Studies, Mysuru, India [2]

Assistant Professor, MCA, VTU, PG Studies, Muddenhalli, Bangalore, India [3]

Assistant Professor, IS&E, VTU, SVIT, Bangalore, India [4]

Abstract: Cloud computing would be one of technologies which is going to play a vital role in the next generation of computer engineering field. The increased scalability and flexibility provided by the cloud computing has reduced the costs to a greater extent and therefore the technology has gained wide acceptance. The facility of Data outsourcing in the clouds enables the owner of the data to upload the data and other users can access the same. But, the data stored should be secure in the cloud servers. The data owner has lot of concern about security aspects present with the cloud computing. The data owners hesitate to adopt cloud computing services because of privacy protection issues of data and security of data. The proposed research work aims to undertake the critical issue of identity revocation wherein outsourcing computation into IBE has been introduced for the first time and a revocable IBE scheme in the server-aided setting has been proposed. This scheme offloads most of the key generation related operations to a Key Update Cloud Service Provider for key-issuing and key-update processes. Only a constant number of simple operations for PKG and users are left to perform locally. Data security is provided by using encryption, user authentication; re-encryption in the proposed data storage security model. The proposed system has also introduced outsourcing computation into IBE revocation, formalizes the security definition of outsourced revocable IBE for the first time to the best of our knowledge. Finally, experimental results have demonstrated the efficiency of the proposed construction.

Keywords: Cryptography, Cloud, IBE

I. INTRODUCTION

Cloud computing is a model which enables the users for storing the data and programs and accessing them easily through an internet instead of using some hardware and software components in the computer. A cloud computing also have many definition based on their different types of models. The cloud models are classified as the deployment and service models. Cloud users will easily access the applications and data content that stored in the cloud from anywhere in the world by the financial model called as pay-as-you-go.

Whenever the data is stored in the cloud there may be problem of security issues and once when the data is outsourced to cloud the cloud provider should check for the data content and the information regarding to the privacy and according to that provided information the provider must provide the security. For the purpose of security different attributes based encryption schemes are used for encryption before outsourcing the data to the cloud server [12].

With authentication and authorization the user can secure the data in the cloud. The data stored in cloud will be usually stored in the pool and where it tries to provide security to those user data content.

A. Outsourcing Data in Cloud

Outsourcing is a familiar method where the third party executes some function for the sake of the company, frequently for the IT department which do not have the resources to undertake. It is an important method for the global information sharing. One of the important services in outsourcing is the database outsourcing during this process the data must be secured from the hackers.

B. Cryptography

Cryptography is a method which is used for storing and transforming the data in the particular form so that only the intended users can read or process the data easily.

Cryptography access control is a commonly used technique for the purpose of securing the data on the entrusted servers. Usually when we use this kind of servers then the sensitive data is encrypted before outsourcing the data and the decryption keys will be given only to the approved users and only by using these keys they can decrypt the data without these keys even the servers are not able to decrypt the data [14].

Cryptography is usually classified into 3 different phase they are as follows:

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

- Secrete key cryptography.
- Public key cryptography.
- Hash function cryptography.

C. Secrete Key Cryptography

A single key will be used by both the user and the receiver here the user contains a key for the data encryption then a similar key will be used by the receiver to decrypt the data hence both users share the same key for encryption and decryption [13].

D. Public Key Cryptography

In this it consists of two keys the one key will be used by the sender and the receiver to secure the data and other key between the receiver and the sender to insecure the provide data content [13].

E. Hash Function Cryptography

In this it does not contain any key pairs instead it uses the hash values which will be processed on the basis of the text message content. It is used to check whether the sent data is not altered by others and the data is not affected by the virus [13].

In cryptography we have various methods:

- Substitution methods.
- Reciprocal methods.
- Symmetric methods.
- Asymmetric methods.

The security for the data can be most commonly done by using the Asymmetric method and this method is also called as the public-key method. In this method the key holder will be provided with two keys the public key and the private key content [13].

F. Encryption and Decryption

For the purpose of securing the data in cloud we use the encryption and decryption methods. The security for the data can also be done using the following phases:

G. Generating the Keys and Authentication Method

Users are said to store their id secretly because it acts as a tool to verify the user every time when they login to the system.

The valid users have some id/password combinations for the purpose of providing the security to their data. The authentication can be done through biometrics were we look into fingerprint, voice face, keyboard timings of the users.

The authentication can also be done by cipher text content. The cipher text is an encrypted text where the data result will be obtained in an encrypted format. The data owner's identification, significance and the key (master/public) of the data owners attributes will be contained in the cipher class content [15].

H. Key Aggregation

When data is shared over the distributed cloud environment it can be secured by providing the aggregate key. For the particular data owners the aggregate key consists of some identity to find the perfect identifier along with the attribute based modules. This key is usually used to share the data between each other using some secret keys in between them.

Key aggregation authorizes the users/data provider to share data with others in a confident way by using some small cipher text expansion, and this text can be provided to each authorized users by providing a single and small aggregate keys.

These aggregate key can be sent to the authorized user through any means of communication mode secretly, the communication mode can be via email, SMS etc. This aggregate key helps the other user to decrypt the data [15].

II. KEY REVOCATION PROCESS

Revocation means recall. By public key infrastructure and Certificate Revocation List (CRL) the revocation operation can be done in cryptosystem. The CRL contains a list of certificate that is revoked. Firmly removing the compromised keys can be done by revocation process. Based on the data owners id the keys/data are revoked in cloud.

When the master key content and the public key content are redefined then the revocation event will be called related to their variable attribute and later by using the master key the data will be re-encrypted [15].

J. Proxy re-encryption and Identity Based Encryption (IBE)

The secure communication can be done in the public key cryptography when both the sender and receiver tries to create a encryption and signature key pairs to the data content that has to be secured and then submit the certificate request to the Certificate Authority (CA) along with the proof of identity and then receive the CA-signed certificate which is used for validation and then later they exchange the encrypted message. This process was time consuming and to out come from this process the identity based encryption was introduced.

This as the following advantage:

1. In IBE system we use strings such as email address or IP address are used for the public key to the user content instead of issuing certificate or revocation keys.

2. Users does not store any additional decryption key in proxy re-encryption, i.e only by using the users own secret keys the decryption process will be completed.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

III. REVIEW OF LITERATURE

The study of R.V. Agalya and K. Karthika Lekshmi [1] works on the ABE (Attribute Based Encryption) used store the encryption data in the cloud. It allows the user to encrypt and decrypt the data by using the attributes. In ABE scheme decryption contains the expensive operations. The elimination of the decryption problem can be done by the ABE system with the outsourced decryption. In this the user data will be submitted to the cloud provider with some transformation key and due to this key content the cloud translates any ABE cipher text attribute to simple cipher text content. Hence in this they introduce an ABE encryption and with the outsourced decryption along with some verification contents and recovery techniques. Hence this technique helps to secure the data and obtain correct data along with the recovery mechanism and avoids the hacking problem from the hackers.

J.Wei et al. [2] proposed a notation called Revocable Storage Identity-Based Encryption (RS-IBE) this provides a forward/backward security of the cipher text content by introducing the functionalities of user revocation and simultaneously the updation of the cipher text will be done. The performance of the proposed system is more advantageous in terms of efficiency and functionality and it is feasible for cost-effective and data-sharing system.

J.Y.Huang et al. [3] they have concentrated on the identity based key management system for the configurable hierarchical cloud computing environment. This proposed system consists of computation on the encryption, authentication and also provides the efficient key reconstruction in case of PKG failures. Due to this facility it reduces the key construction cost on cloud computing data centres.

S.Qui et al. [4] they have studied the problem about the private matching over the outsourced encrypted datasets in the identity based cryptosystem and this can be simplified by the certificate management. So they have proposed an Identity Based Private Matching Scheme (IBMP) which enables the cloud server to perform the private matching operations without any leakage of the private data content. They analysed the data through the asymptotic complexities and with the experimental results they found that the cost of the IBPM was linear to the size of dataset and it is also more efficient then the existing system which was proposed by Zheng [30]. So in this system they try to include two things for better matching they are the identity-based fuzzy private matching and the identity-based multi-keyword fuzzy search.

Y.M.Tseng et al. [5] the author Li.et al as proposed a revocable IBE (Identity Based Encryption) scheme with a Key Update Cloud Service Provider (KU-CSP) hence it as many drawbacks so the proposed system contain a new revocable IBE scheme with the Cloud Revocation Authority (CRA) to solve two problems that is where the performance will be improved and the CRA holds only the system secrete for all the users. And for the security the proposed system will provide a similar secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Hence these proposed systems contain the CRA-aided authentication scheme for managing a large number of various cloud services.

Jin Li et al. [6] works on the encryption and decryption process using some standards as the Data Encryption Standard (DES). DES is also called as the data encryption algorithm. It is a kind of block cipher where the data will be encrypted into a mass of 64 bits each and DES uses these bits as input and it is obtained by 64 bits of cipher text. In this algorithm they use some keys for encryption and decryption process. Hence the key length will be 56 bits. This algorithm is based on substitution (confusion) and transposition (diffusion) attributes. DES contains 16 steps; every step is called as a round. The steps of substitution and transposition are performed at every round. C.Wang et al. [7] studied about the image data sets and the way to secure the sensitive data that is outsourced and hence they proposed the Outsourced Image Recovery (OIRS) which concentrates on some of the aspect from the starting of the service flow the aspect are like securing, competence, and design complexity. In the proposed system the data owners not only outsource the compacted image content to the cloud but also reconstruct the images without enlightening its details from the corresponding samples of the image content.

Li et al. [8] in this they work on the map reduce cloud of ABE which helps in providing the the data is outsourced the cost of the user will be reduced during the encryption process. The advantage of this system is the user will be able to delegate the encryption content for any different policy content.

M.Green et al. [9] works on ABE in this they try to reduce the user burden while using the cipher text that are stored in the cloud. In this they provide a single transformation key to the users and this key allows the cloud to translate any kind of the ABE cipher text into an El Gamal style cipher text content without the cloud is able to read the any part of the user message content. Apart from this it also helps in providing the security by using the security definition like the CPA and the repayable CCA security for the outsourced data. Varsha S.Agme and Archana C.Lomte [10] they work on enhancing the data security model which is done using the cloud services. The proposed system tries to provide security to the data using the three steps they are as follows firstly the data encryption will be done next the data has to be decrypted so the decryption is done by using the user authentication after obtaining the user authentication details then the data will be decrypted to those users. Apart from this process it also provides the protection against the threats and formally known as DDOS attacks. This system also provide a facility to the user in which the user can request

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

for the information by sending a SMS and it is not necessary to be in online always. Kiran et al. [11] studies about the image processing technique they try to work on the unsharp masking technique. They provide security to the data by increasing the security levels for the encoded encrypted images. They try to use only a single key for the purpose of encryption and decryption of those images. Apart from this they have also used the compression technique for its better compression. Finally some experiments are conducted to check whether the image is secured in the network.

IV. PROPOSED SYSTEM & ARCHITECTURE

In this proposed system we represent a model for the outsourced revocable IBE by using the system architecture which has been compared with IBE scheme. For the compromised users the revocation will be realized by the KU-CSP. It is treated as a public cloud which will be run by another party to provide the capability of computing to PKG for regulating the network by using the services. The KU-CSP is given away from the users or the PKG, this PKG helps to reduce the storage cost and estimation of the users only by giving the flexibility and also the temporary extension to the user infrastructure. When the revocation process is activated the private keys is not re-requested from the PKG the unrevoked users of this system must ask the KU-CSP for updating a small component of their secrete key content. In the KU-CSP's deployment it contains many informative details but here we only visualize it as a service provider, and concentrate on the way of designing it for the purpose of securing the users data with an unreliability KU-CSP. Further it consists of three requirements for such model the requirements are as follows:

1. Any one of the KU-CSP must be honest
2. There might be the computational complexities, so to obtain the effect to the revocation a true KU-CSP is needed.
3. The PKG run time might be much smaller than needed to directly act or carry out revocation process.

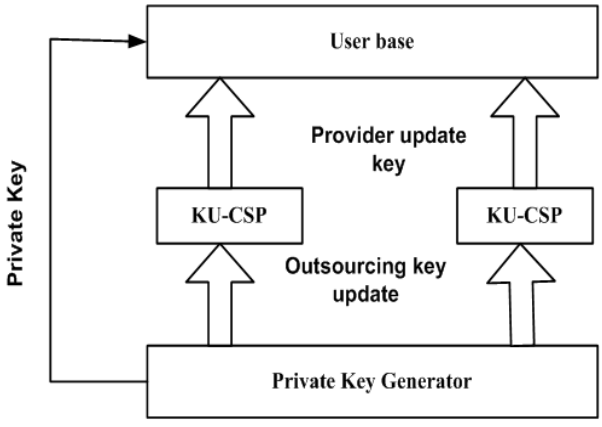

Fig 1 Architecture of Proposed System

The system architecture provides the information about the system along with its related contents. It is a conceptual model and hence this model provides information regarding the behaviour, working etc. The below architecture shows the task done by the particular system:
In the above provided architecture it helps to obtain the work of the proposed system. In this architecture the PKG generates a private key to the user and they will be provided by the private key/secrete key and the outsourcing key will be provided to the KU-CSP and the KU-CSP stores the outsourcing key. When the user needs for updation of keys they can update the keys easily with the KU-CSP instead of going back to PKG.

V. RESULT & ANALYSIS

Fig 2: Admin login Page

Shows the admin login page, wherein the administrator takes care of the user registration.

Fig 3: User registrations Page

After the successful admin login, admin can register user by clicking on User button which directs to above registration page where user details are provided.

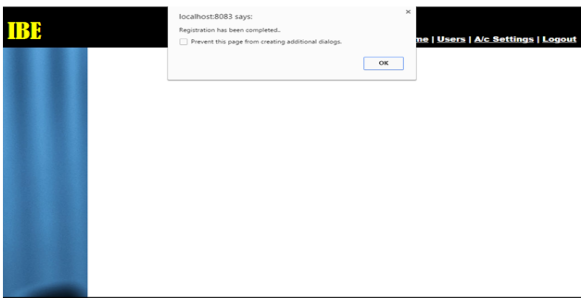

Fig 4: Registration Acknowledgement

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

Above figure shows the registration acknowledgement for successful user registration by the admin.

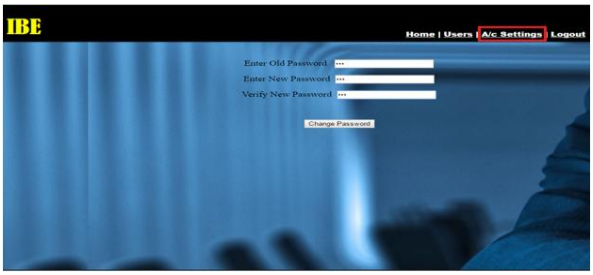

Fig 5: Admin account setting

Above figure shows the admin password changing page, in order to enter into this page click on A/C Settings button and provide old and new password to change the existing password.

Fig 6: Admin password change acknowledgement

Above figure shows the acknowledgment for the password change by the admin.

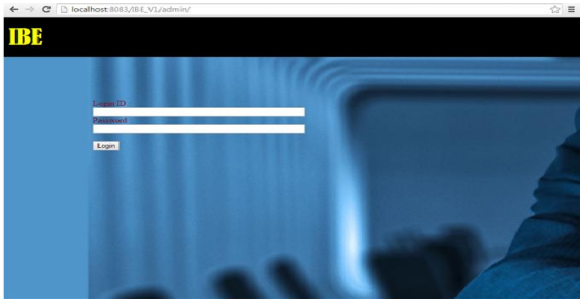

Fig 7: Admin login Page

Above figure shows the login page for the admin using the new password.

Fig 8: Login Page for Registered user

Above figure shows the login page for the registered user.

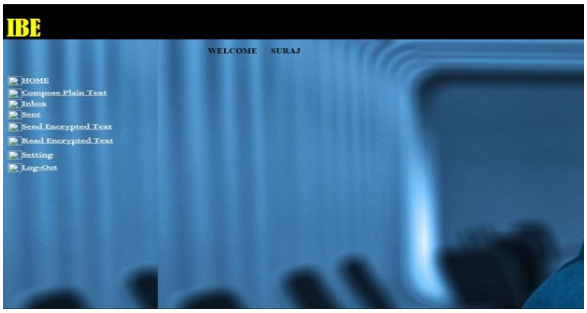

Fig 9: Registered User welcome page

Above figure shows the Welcome page for the registered user.

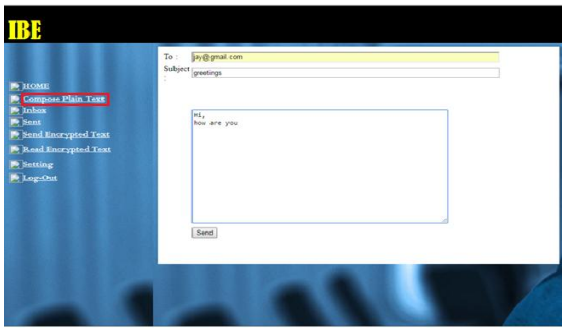

Fig 10: User composing Plaintext

Above figure shows the user composing a plain text mail by clicking on the compose Plain text button.

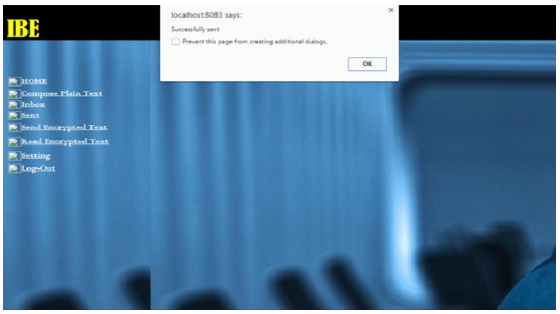

Fig 11: Acknowledgement of delivery

Above figure shows the acknowledgement message for successful delivery of plaintext message.

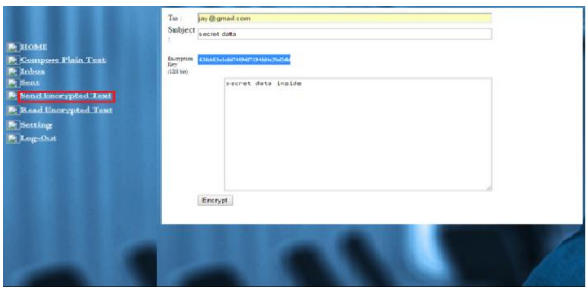

Fig 12: Sending encrypted message

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

Above figure shows the user composing secret message to send it to another user. This message is composed by clicking on send encrypted text button.

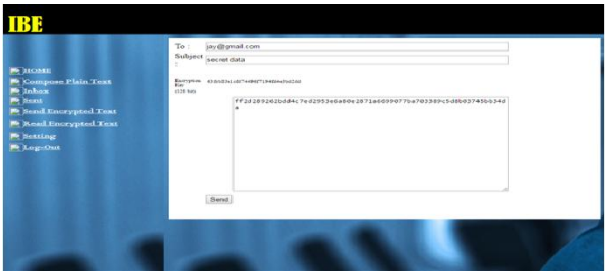

Fig 13: Encryption of the secret message

Above figure shows the encrypted version of the secret message, the encryption is performed using 128 bit key.

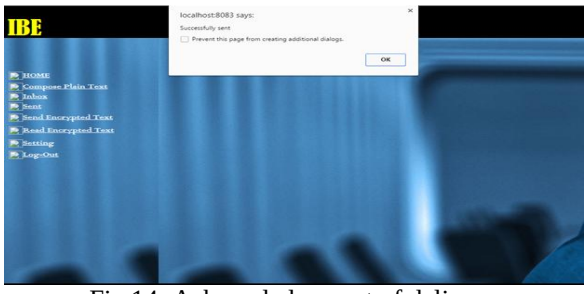

Fig 14: Acknowledgement of delivery

Above figure shows the acknowledgement message for successful delivery of cipher text message.

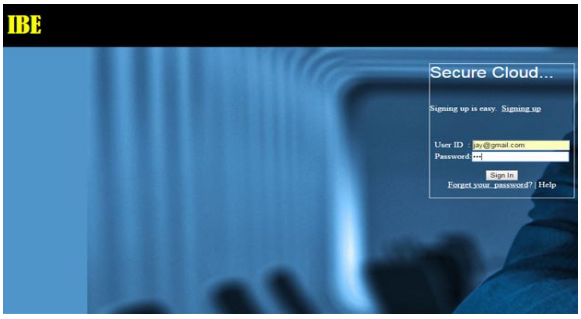

Fig 15: Receiver user login

Above figure shows the login page of the receiver user.

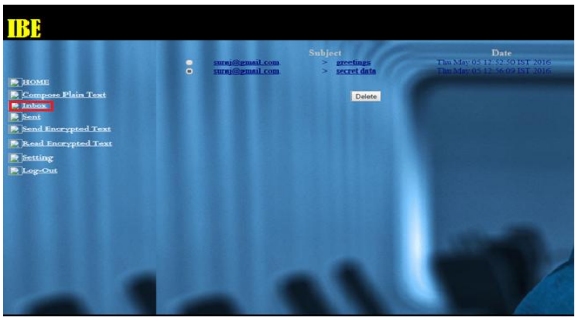

Fig 16: Receiver user page

Above figure shows the receiver user page, where by clicking on the inbox button we check the received mails.

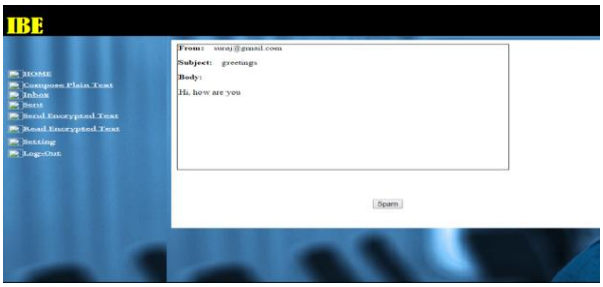

Fig 17: Plaintext received by the receiver user

Above figure shows the plaintext message received by the user, click on desired message on the inbox to open it.

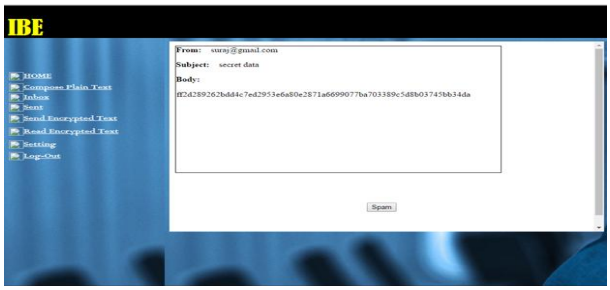

Fig 18: Encrypted text received by the receiver user

Above figure shows the encrypted text message received by the user, click on desired message on the inbox to open it. This message contains the encrypted form of secret message.

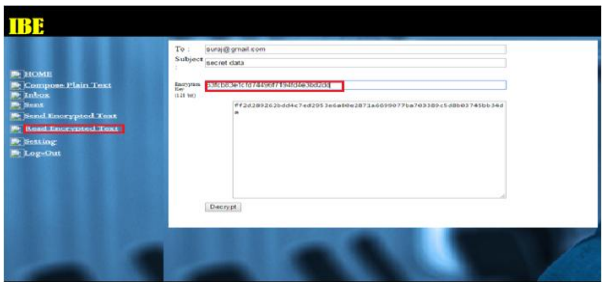

Fig 19: Decryption of the encrypted message

Above figure shows the decryption of the secret message using the 128 bit encryption key.

Fig 20: Decrypted secret messages

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

Above figure shows the decrypted secret message received in the receiver user inbox.

V. CONCLUSION

Cloud computing is a distributed system connected with the servers where users can share data each other. An Identity-based proxy re-encryption scheme has been introduced to outsource the sensitive data from the main user to the external user. Nevertheless, they cannot be employed in cloud computing.

This system will increase the security by introducing the identity based secure encryption and re-encryption process for the stored data. This work has concentrated on the identity revocation. It has used outsourcing calculation in the IBE and suggested in a revocation scheme where in the revocation operation is delegated in CSP. The proposed system achieves the following:

1. It provides constant efficiency to compute the PKG and size of private key at the user.
2. It offers convenience since the user may not contact the PKG at the time of key updation and there is no need of user authentication between the user and the CSP.

REFERENCES

[1] Agalya, R. V., and K. Karthika Lekshmi. "A Verifiable Cloud Storage using Attribute Based Encryption and Outsourced Decryption with Recoverability."
[2] Wei, Jianghong, Wenfen Liu, and Xuexian Hu. "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption."
[3] Huang, Jyun-Yao, I-En Liao, and Chen-Kang Chiang. "Efficient identity-based key management for configurable hierarchical cloud computing environment."Parallel and Distributed Systems (ICPADS), 2011 IEEE 17th International Conference on. IEEE, 2011.
[4] Qiu, Shuo, et al. "Identity-Based Private Matching over Outsourced Encrypted Datasets."
[5] Tseng, Yuh-Min, et al. "Identity-Based Encryption with Cloud Revocation Authority and Its Applications."
[6] Wang, Cong, et al. "Secure ranked keyword search over encrypted cloud data." Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010.
[7] Wang, Cong, et al. "Privacy-assured outsourcing of image reconstruction service in cloud." Emerging Topics in Computing, IEEE Transactions on 1.1 (2013): 166-177.
[8] Li, Jingwei, et al. "Outsourcing encryption of attribute-based encryption with mapreduce." Information and Communications Security. Springer Berlin Heidelberg, 2012. 191-201.
[9] Green, Matthew, Susan Hohenberger, and Brent Waters. "Outsourcing the Decryption of ABE Ciphertexts." USENIX Security Symposium. Vol. 2011. No. 3. 2011.
[10] Agme, Varsha S., and Archana C. Lomte. "Security Enhancement of Outsourced Data on Cloud Using Identity Based Encryption." (2014).
[11] G. Thippanna, Dr. T. Bhaskara Reddy, Dr. S. Kiran , " Image Masking and Compression Using user Private Key Generation" , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) , Volume 3, Issue 5, September - October 2014 , pp. 262-266 , ISSN 2278-6856.
[12] Shawish, Ahmed, and Maria Salama. "Cloud computing: paradigms and technologies." Inter-cooperative Collective Intelligence: Techniques and Applications. Springer Berlin Heidelberg, 2014. 39-67.
[13] Thippanna, G., T. Bhaskara Reddy, and S. Kiran. "Image Masking and Compression Using user Private Key Generation." IJETTCS ISSN: 2278-6856. [14]Swarup kshatriya and Dr.Sandip M Chaware. A Survey on Data Sharing using Encryption technique in cloud computing.
[15] R. Subbu lakshmi and R. Nirmala Survey on Imparting Data in Cloud Storage Using Key Revocation Process.
[16] http://www.cloud tutorials.com.
[17] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou Identity-Based Encryption with Outsourced Revocation in Cloud Computing.
[18] Jianghong Wei ; Wenfen Liu ; Xuexian Hu Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption
[19] Geetanjali P. Rokade , Sambhaji Sarode Survey on Implementing Privacy Preserving Model for Shared Data in The Cloud.
[20] Dr.V.VENKATESA KUMAR , M.NITHYA , Mr.M.NEWLIN RAJKUMAR An Assessment on Identity Based Encryption Mechanisms in Cloud Computing
[21] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, "Towards Secure and Dependable Storage Services in Cloud Computing"