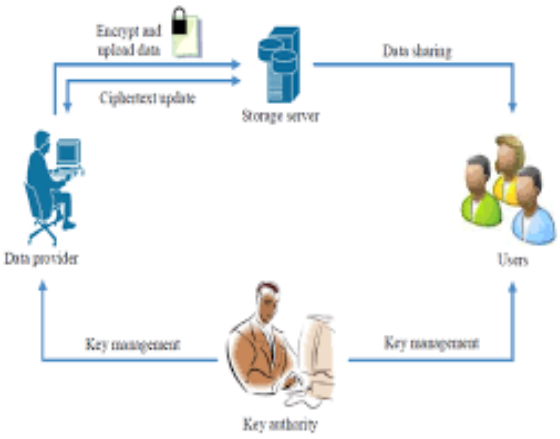
Secured Cloud Computing Using Identity Based Encryption

Ms.B.Madhuranjani[1], B.Kousalya Devi[2], E.sureshkumar[3], Nadjib youssouf mondoha[4]
[1, 2, 3, 4] Dept of computer science
[1, 2, 3, 4] Sri Krishna arts and science college, Coimbatore -641 008.

Abstract- *Cloud computing is a concept of paradigm which provides enormous computation capacity and huge memory space at a low cost. It brings great convenience to cloud users which enables cloud users to consider services regardless of time and location across multiple platforms (e.g., mobile devices, personal computers). Thus, it's necessary to put cryptographically increased access management on the shared knowledge. Identity-based cryptography could be a promising cryptographically primitive to create a sensible knowledge sharing system. However, access control is not static. That is, once some user's authorization is invalid, there should be a mechanism that can remove him/her from the system. By that the removed user cannot access both forward and backward data. For this we use a concept called revocable-storage identity-based encryption (RS-IBE), which provides security of cipher text for forward/backward data by introducing the user revocation functionalities and simultaneous update of cipher text. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the security model. The performance comparisons indicate that the planned RS-IBE theme has benefits in terms of practicality and potency. Finally, we provide implementation outcome of this suggested scheme to define its feasibility.*

I. INTRODUCTION

Cloud computing provides a legible and convenient means for information sharing, that brings varied beneath for each the society and people. But there exists a natural resistance for users to directly supply the shared info to the cloud server since data} typically contain valuable info Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility.ID-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based cryptography. Because a type of public-key encryption user of public key has some unique information about the user identity (e.g. email address of user). This means that a sender World Health Organization has access to the general public parameters of the system will code a message victimization e.g. the text-value of the receiver's name or email address as a key. From the central authority the decryption keys are obtained to the receiver, which needs to be trusted as it generates secret keys for every user. By knowing the ASCII string in system of Identity Based allow to generate a public key by known identity value by any party[6]. Corresponding private keys are generated by trusted third party, called the Private Key Generator (PKG). In order to corresponding private key are to be obtain, identity ID contacts the PKG used by the party authorized , to generate the private key for identity ID which uses the master private key.



Outsourcing information to cloud server implies that information is out management of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information [5]. Even worse, cloud server itself might reveal users' information for contraband profit. Data sharing is not static. When the authorization of user is expired, he/she could not access the previously and subsequently shared data [9]. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data [11]. A solution to overcome the problem is to use access control such as identity-based encryption (IBE).

CLOUD SECURITY

Identity-based access control placed on the shared data should meet the following security goals: Data confidentiality: Plaintext of the shared data stored in the cloud

server should be prevented from accessing the data by unauthorized users.

Backward secrecy: Secrecy on Backward means , when the authority of user's was expired, or secret key of user was compromised, Previously accessed data by him/her should be prevented from accessing the plain text of shared knowledge by underneath identity of his/her the later on shared knowledge of plain text are still encrypted[12] .

Forward secrecy: Secrecy on forward suggests that, when the authority of user's was expired or secret key of user was compromised. Under identity of his/her the subsequently shared data of plain text are still encrypted [1].

RIBE OPERATION

The identity-based encryption concept is introduced by Shamir, and conveniently instantiated by Boneh and Franklin. IBE eliminates the need for providing a public key infrastructure (PKI).

II. SYSTEM ANALYSIS

EXISTING SYSTEM: Non revoked users are proposed in IBE from the way of natural revocation in which the private keys are periodically received all time from key authority. Since, the solution is not stable, the non –revoked users requires the authorization of key to perform linear work [14].

Natural revocation way for IBE is first proposed by Franklin and Boneh.

To achieve efficient revocation an approach was produced by Goyal, Boldyreva and Kumar. They used a binary tree to manage identity such their RIBE theme reduces the complexness of key revocation to exponent (instead of linear) within the most variety of system users [10].

DISADVANTAGES OF EXISTING SYSTEM:

It's not scalable.
It's not secure.

PROPOSED SYSTEM

To overcome the existing system introduce a approach a notion called revocable storage identity-based encryption (RS-IBE) in order to build data sharing system by cost effective that fulfills the three security goals. • We provide formal definitions for RS-IBE and its corresponding security model [10]. • We present a concrete construction of RSIBE. The projected theme will offer confidentiality and backward/forward2 secrecy at the same time. • By using the ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) dimension, we prove the security for the proposed model. In order, the proposed scheme can withstand decryption key exposure.
ADVANTAGES OF PROPOSED SYSTEM: The procedure of cipher text update only needs public information. By the forward secrecy additional computation and storage complexity was brought.

III. RELATED WORK

Revocable identity-based encryption

Public key and private key are used to encryption and decryption respectively in this paper, normally forward secrecy or backward secrecy provided for security. In this paper, Forward secrecy is employed for advanced security. Revoke user can't access the previous or subsequent data so that revocable identity based encryption technique is used. Data suppliers transfer the files into storage server victimization the cryptography technique. For the encryption key is used and this key provide by the key authority. Key authority is responsible for sending the key to data provider [11]. In this paper, random function used for generating the key to encryption as well as decryption. Storage server stores the files that ar uploaded by information supplier. And users transfer or access the file as per their want. Download the file is done through decryption process

Key Authority

Firstly for downloading file key will be send and this key is send again key authority. If key will be match between data provider and user then user will authorized to download the data. Else key does not match then the user cannot download the file. After matching key OTP will be send to the user. At this stage, time limit should be provided because of more security for accessing the data using cloud computing. Within a time period user can type the OTP. If OTP is type within time then user can access this file. Else time period is expired then user cannot access this file. And one more condition is that, if OTP is wrong then user enters into revoke list[9][11]. In this system initial knowledge supplier transfer the file. And upload file convert into the encrypted format using key encryption algorithm. I.e. AES algorithm. Then storage server accountable not solely storing the information or files however, also give permission for unrevoked user to access the data or files through cloud computing. User send request for accessing data permission to data provider via storage server [8]. Then key authority generates the key as per

user requested data. These generated key is send to user. After receiving key, data provider key and user key will be match. If key will be match then user is authorized to download the data. Else it cannot the file. After matching of key again OTP will be send to user for extra security. User can write the OTP within time period. Again user will write the OTP within a time period. Then user can download the required file successfully. Else it cannot download the needed file. This whole process provide large security in cloud computing. In this paper, extra security for data sharing in cloud computing should be provided. There for sharing data through cloud computing is securely [11].

IV. MODULES

System Construction Module:

In this first module, the proposed system was developed with the required entities for the evaluation of the proposed model. The user was first decided by the data provider who can share the data. Then, Data provider encrypts the data under the identities user, and uploads shared data of cipher text to the cloud server. When users want to get the shared data, she/ he can download and decrypt the corresponding cipher text. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available [1].

Data Provider

In the second module, Data Provider module was developed. The development of data provider module is for which the new users will Signup first and then Login for authentication. By here the data provider module provides the option of uploading the file to the Cloud Server [6]. By using Identity-based encryption format the process of File Uploading to the cloud Server is undergone. He / she can check the progress status of uploading the file. Data Provider provided with the features of Revocation and Cipher text update the file. Once the process is completed, the Data Provider can logouts the session.

Cloud User

In this module, Cloud User module was developed. The Cloud user module is developed specified the new users can Sign up at the start so Login for authentication. The file search option will be provided by the Cloud user [13]. Then cloud user feature is extra up for send the Request to Auditor for the File access. After getting decrypt key from the Auditor, he/she can access to the File. The cloud user is additionally enabled to transfer the File. After completion of the process, the user logout the session[1][5].

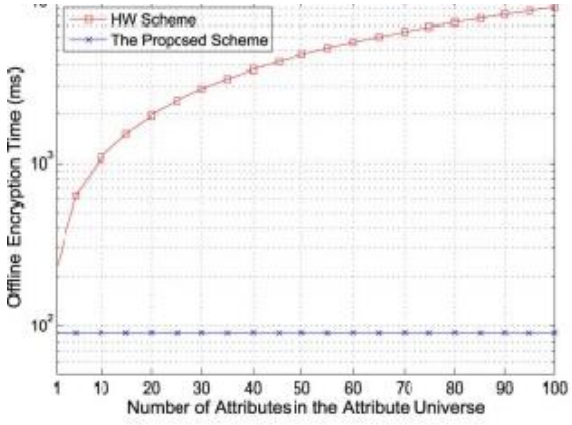
Key Authority (Auditor)

Auditor's page will be log in by the auditor. He/she will check the pending requests of any of the above person. After accepting the request from the higher than person, he/she will generate master key for encrypt and secret key for decrypt [5][8].After the whole method, the Auditor logout the session.

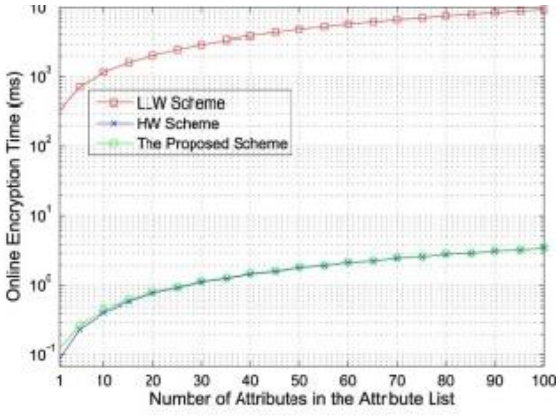
V. RESULT

The results show the graph of the proposed system and the existing system [9][11]. And it shows the time complexity of offline and online encryption. And the result shows the Cost of the Encryption.

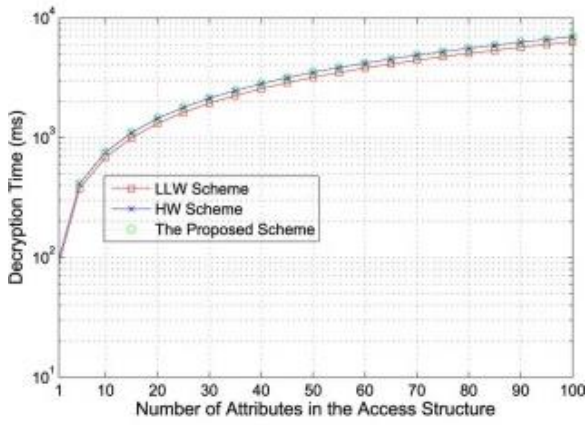
Graph Representation



(a) The offline encryption cost



(b) The online encryption cost



(d) The decryption cost

VI. CONCLUSION

Cloud computing has many advantages such as space of storage is increased and cost of storage is reduced and decreases overheads on cloud, storage security . Proving the security to the data placed in cloud computing has become major issue in this IT platform [1]. This paper mainly concentrates on security and privacy issues and also discusses about the different techniques used in existing cloud environments. Further, these different techniques are used in improving the security of the data stored and also giving privacy to the data [5][8][9].

REFERENCES

[1] Jianghong Wei, Wenfen Liu, Xuexian Hu-IEEE Transactions on Cloud Computing (Volume: PP, Issue: 99) March 2016

[2] Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[3] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially driven resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[4] Kishore Babu V, 2R Amutha http://www.ijsdr.org/papers/IJSDR1706010.pdf

[5] B. Wang, B. Li, and H. Li, ―Public auditing for shared knowledge with economical user revocation within the cloud,‖ in INFOCOM, 2013Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[6] DrAnanthi Sheshasaayee, 2R. Megala, "A Conceptual Framework For Resource Utilization In Cloud Using Map Reduce Scheduler" International Journal of Innovations in Scientificand Engineering Research (IJISER), Vol. 4, No.6, pp.188-190, 2017.

[7] S. Ruj, M. Stojmenovic, and A. Nayak, ―Decentralized accesscontrol with anonymous authentication of data stored in clouds,‖Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2,pp. 384–394, 2014.

[8] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, ―Costeffective authentic and anonymous knowledge sharingwith forward security,‖ Computers, IEEE Transactions on, 2014, doi:10.1109/TC.2014.2315619.

[9] Mohan, Prakash, and Ravichandran Thangavel. "ResourceSelection in Grid Environment Based on Trust Evaluation usingFeedback and Performance." American Journal of AppliedSciences

[10] 10.8 (2013): 924. 10. Prakash, M., and T. Ravichandran. "An economical Resource Selection and Binding Model for Job designing in Grid."European Journal of research eighty one.4 (2012): four50-458.

[11] Jin Li (School of Computer Science, Guangzhou University,Guangzhou, China),Wenjing Lou (Virginia Polytechnic Institute and State University, Blacksburg) "Identity based encryption with outsourced revocation in cloud computing" 2015.

[12] Prakash, M., R. Farah Sayeed, S. Princey, and S. Priyanka."Deployment of MultiCloud Environment with Avoidance of DDOS Attack and Secured Data Privacy." International Journal of Applied Engineering Research 10, no. 9 (2015): 8121-8124.

[13] Annamalai, R., J. Srikanth, and M. Prakash. "Integrity and Privacy Sustenance of Shared giant Scale pictures within the Cloud by Ring Signature."International Journal of pc