

Enhanced Data Security Protection Mechanism for Cloud Storage using Two Factor's.

Thite Amruta S.¹, Dere Sarika B.², Rohakale Shital D.³, Kalekar Namarta Y.⁴

¹ Thite Amruta S., Computer Dept., SGOICOE, Belhe, Maharashtra, India

² Dere Sarika B., Computer Dept., SGOICOE, Belhe, Maharashtra, India

³ Rohakale Shital D., Computer Dept., SGOICOE, Belhe, Maharashtra, India

⁴ Kalekar Namarta Y., Computer Dept., SGOICOE, Belhe, Maharashtra, India

ABSTRACT

This system proposed an improve data security protection mechanism for cloud using two components. In this system sender sends an encrypted message to a receiver with the help of cloud system. The sender requires to know identity of receiver but no need of other information such as certificate or public key. To decrypt the cipher text, receiver needs two parts. The first thing is a unique personal security device or some hardware device connected to the computer system. Second one is private key or secrete key stored in the computer. Without having these two things cipher text never decrypted. The important thing is the security device lost or stolen, then cipher text cannot be decrypted and hardware device is revoked or cancelled to decrypt cipher text. The efficiency and security analysis show that the system is secure as well as practically implemented. The system uses a new hardware device like pen drive etc.to decrypt the cipher text together with the private key.

Keyword: - Cloud storage, Security, Two-Components, factor revocability.

1. INTRODUCTION

There are so many benefits, to store the data in the cloud storage. Data accessed in the cloud storage server can be hosted at any time and any place or anywhere as long as network access. Cloud service provider gives services to the cloud users, they can get any amount of more resources any time. It provides no risk of data Storage maintenance tasks, such as acquiring additional storage capacity, can be unloaded to the responsibility of a service provider. Very easy to data sharing between many users. If sender wants to share a piece of data such as video, text, audio etc. To receiver, it may be difficult for sender to send it by email due to the size of data. Rather than, Alice uploads the file into the cloud storage after that receiver can easily download anytime from any place.

Cloud storage typically refers to an offer object storage services like Microsoft Azure and Amazon S3 Storage. There are different significant challenges in cloud computing for securing data, provision of services and storage of data in the internet from different types of attacks. Cloud computing provides an including space for data storage, computer processing power, shared pool of resources, networks, user applications and specialized corporate. Cloud computing is a more sophisticated. It is easy to forecast that the security for data protection in the cloud storage should be improve. In any cases, these applications go through a potential risk about component revocability that may limit their possibility. An expandable and flexible Two-Component encryption mechanism is really more appropriate in the term of cloud computing that prompt our System.

Cloud computing is a common term for anything that involves scalable services, delivering hosted services like accessing, data sharing, etc. over the web on demand basis. Generally, user share various types of documents through cloud storage networking application like Drop box, cloud me, Google drive. Citrix Cloud computing is known as an alternative to traditional technology due to its low-maintenance and better resource-sharing capabilities. The main goal of cloud computing is to provide high performance energy of computing for various field like military and research organization for performing billions of computations. The essential security requirement can be attained by combining both the cryptographic cloud storage along with searchable encryption scheme. In cloud

system overall cost of data storage is less as it does not require managing and maintaining expensive hardware. In which data owner firstly encrypt all data before storing on a cloud in such way that only user whom having decryption keys can be decrypt or fetch the data.

2. LITERATURE SURVEY

In this paper, propose a two-factor data security protection mechanism with factor revocability for cloud storage system. System allows a sender to send an encrypted files or messages to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver. The receiver needs two parts in order to decrypt the cipher-text. The first thing is a unique personal security device which connects to the computer. The second thing is his/her secret key stored in the computer. It is impossible to decrypt the cipher-text without either piece. More importantly, once the security device is stolen or lost, this device is revoked. To change the existing cipher-text to be un-decryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher-text at any time [1]. This paper gives the information about characteristic of low maintenance. Cloud computing provides financially and efficient solution for sharing data group resource among cloud users, the scheme is also very flexible, it can be simply extended to support more advanced searching query. We conclude that this provide a tremendous building block for the construction of secure services in the cloud storage which are not trusted by user. As we will share only single key the storage space required will become less and more efficient [2].

This paper focuses on trace out data for security concern. Using a log based audit services that concentrate on privileged data utilizer and also consider their time period of utilization for this instance data trace out in the cloud storage. This system overcome various operations on data, also repeated creation of tag and sampling [3]. In proposed cloud storage systems is used to stored cipher-text existing access control strategy are no longer useful, drawback ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a technique for access control of encrypted data [4].

In this scheme presents cryptographic cloud storage based on attribute-based cryptosystems and a new keyword search notion: fine-grained access control aware keyword search. In this system first Group the decryptable files of users before executing the keyword search. It decreases information leakage from the query process. Many system uses the straightforward search approach where for searching one encrypted keyword, the cloud server must look round all encrypted files on the storage to compare that encrypted keyword to each keyword index, this drawback is removed [5]. In focus on problem of Identity-Based proxy re-encryption, in which cipher-text are convert into one identity to another. proxy re-encryption scheme is used to convert the encrypted cipher-text into decrypted cipher-text without in behalf of underlying plaintext. This drawback removes in Inter-domain identity-based proxy re-encryption [6].

The authors share data and privacy preserving auditing scheme with large groups in the cloud. They are utilizing group signature to compute verification information on shared data. That is the TPA those able to audit correctness of shared data but cannot reveal the identity of the signers on each block. The original user can efficiently add new users to the group and close the identities of signers on all blocks [7]. This paper describes a system Identity Based Encryption in standard model and has distinct drawback of existing system such as namely, computation capability, less public framework and a compact safety reduction. Stronger assumption is based on private key generation quires made by attacker.to reduce this drawback using Bilinear diff-hellman Exponent assumption [8].

3. EXISTING SYSTEM

Now a days Cloud storage is known as a promising solution for providing convenient, universal, and on-demand access to greater amounts of information shared on the Internet.

In existing system, they introduced a two-factor security protection mechanism for data stored in the cloud. System is based on Identity-Based Encryption (IBE) mechanism. The sender requires only the identity of the receiver to send an encrypted data. Sender send cipher-text through the cloud to the receiver then receiver can download cipher-text at any time. Existing system accommodate two-factor data encryption protection technique. Encrypted data stored in a cloud, receiver accessed encrypted data and convert into decrypted data that time it will required two

things: First thing, user secret key which is send by sender through a secure channel (e.g., email). Second thing, user needs unique personal security device to connect the computer such as USB.

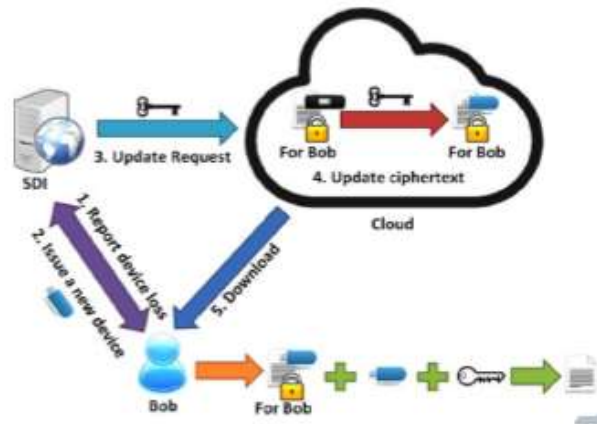


Fig. Architecture of Existing System

The system user required a security device then it will request for security device to the security device issuer (SDI) suppose device is theft or loss then user report to SDI, after that issuer revoked personal security device of user and afford a new unique or personal security device to user.

3. PROPOSED SYSTEM:

This paper focuses on an improve data security protection mechanism for cloud storage using two components. Before giving the description of the system, firstly we will give a prior knowledge on it. A proposed system provides following objects:

- **Security device Account Manager (SDAM):** It is an ethical party responsible for issuing unique security device of each user.
- **Sender (Bob):** Sender is a creator of the cipher-text. Sender uploads encrypted file on to the cloud storage system.
- **Receiver (Alice):** She as a receiver download the encrypted file(cipher-text) which is stored on cloud server, and decrypt the downloaded file.
- **Cloud Storage:** All encrypted file sender to upload, the uploaded file is stored on to the cloud storage. All storing responsible is depend on cloud server (for receiver to download).

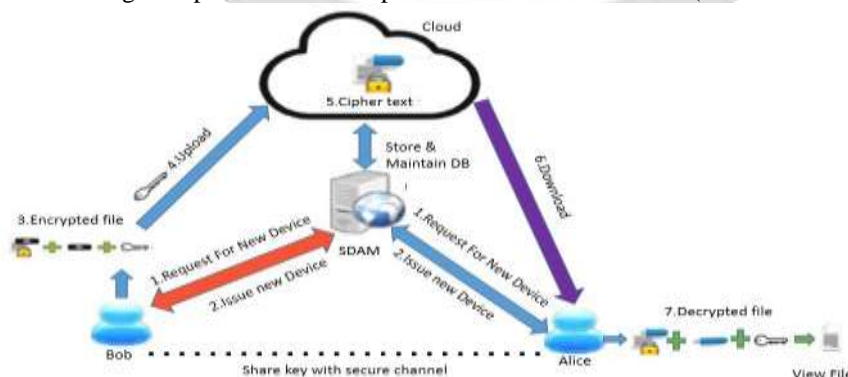


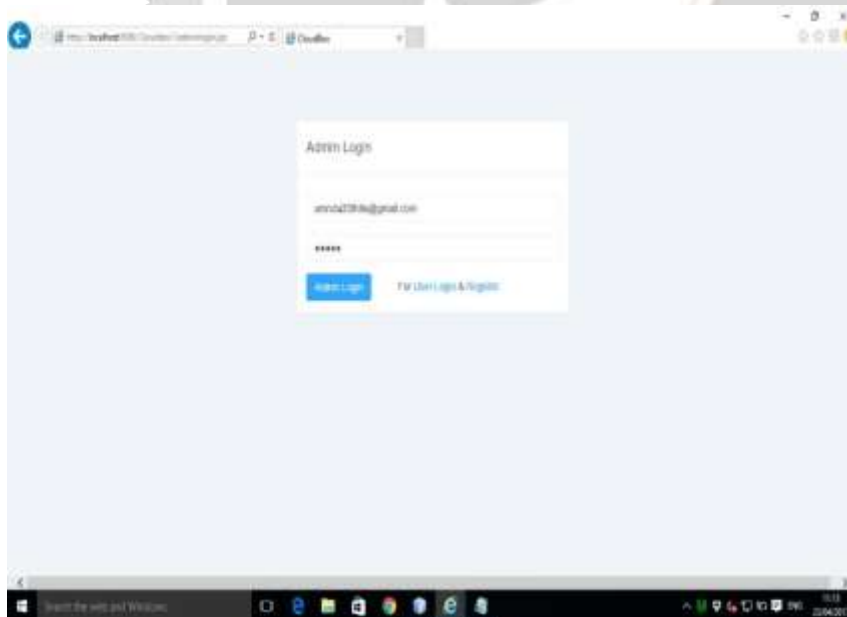
Fig. Architecture of Proposed system

In this system, every user required a registration first, that time he/she send your details to a SDAM. The SDAM will verify whether user is valid or not as per user details, after the verification user purchasing a unique security device which is provide by a SDAM. First user sends a request to the SDAM for issuing a device, then SDAM will verify whether user is valid or not as per user details, after the verification if user is valid then SDAM will assign a security device to that user. Sender transfers some file to receiver side in an encrypted format. The cipher-text store on cloud storage, but before uploading a files he/she is the sender who convert the original file or data into an encrypted format. Sender requires a two thing- first thing is the unique personal security device and second thing is secret key. then original file convert into encrypted format and file will upload to the cloud. At sending time sender requires only the identity of a receiver, no other information requires such a public key, certificates, signature etc. sender generate a secret key which is send through secure channel to receiver.

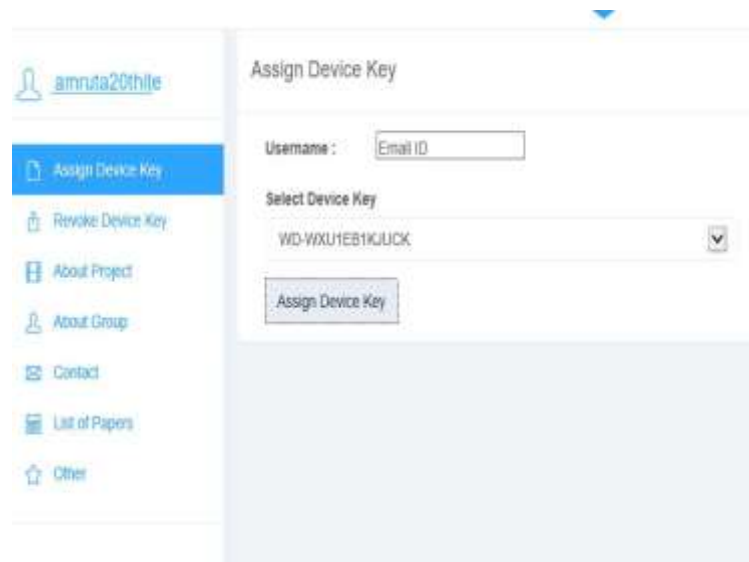
Responsibility of cloud system is to store encrypted file for a downloading to a receiver. At receiver side, receiver will download the encrypted file which is stored on cloud. Receiver requires a two thing to convert encrypted file into decrypted format. first thing is the unique personal security device and second thing is secret key. Only with the help of this two things receiver can decrypt the encrypted file which is downloaded from cloud server. If device is stolen or loss, then user should report to SDAM first. After this SDAM revoked personal security device of user and afford a new unique or personal security device to user.

OUTPUT:

[1]



[2]



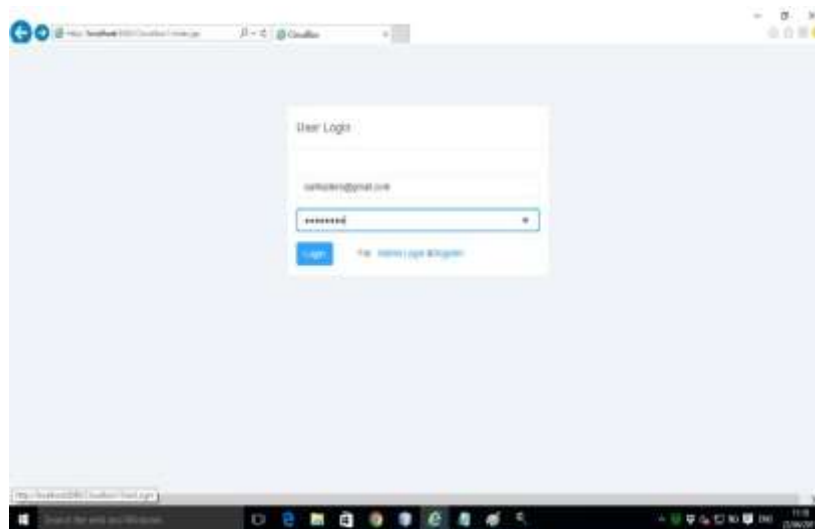
The screenshot shows a web application interface for assigning a device key. On the left is a sidebar menu with the user profile 'amruta20thile' at the top. The menu items are: 'Assign Device Key' (highlighted in blue), 'Revoke Device Key', 'About Project', 'About Group', 'Contact', 'List of Papers', and 'Other'. The main content area is titled 'Assign Device Key' and contains the following fields: a 'Username' field with 'Email ID' entered, a 'Select Device Key' dropdown menu showing 'WD-WXU1EB1KJUCK', and an 'Assign Device Key' button.

[3]



This screenshot shows the same 'Assign Device Key' web form as in [2], but with a green success message at the top: 'Device Key Assignment Successful Your DeviceKey is WD-WXU1EB1KJUCK'. The form fields and sidebar menu remain the same. The browser's address bar shows the URL 'http://192.168.1.100/CloudBox/assignDeviceKey.aspx'. The Windows taskbar at the bottom indicates the system time is 10:16 on 10/10/2017.

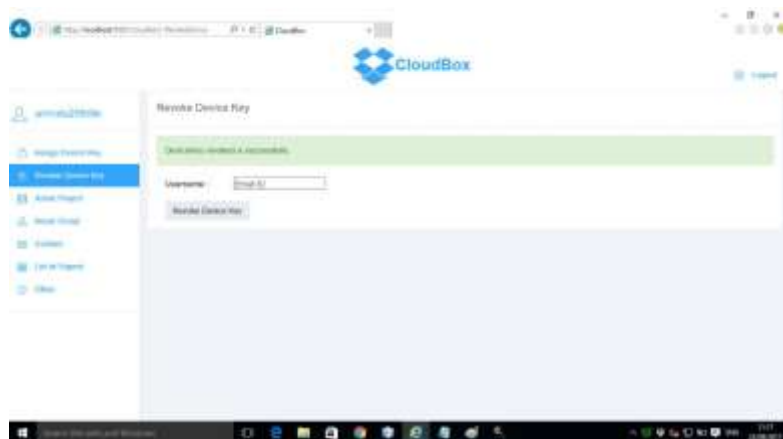
[4]



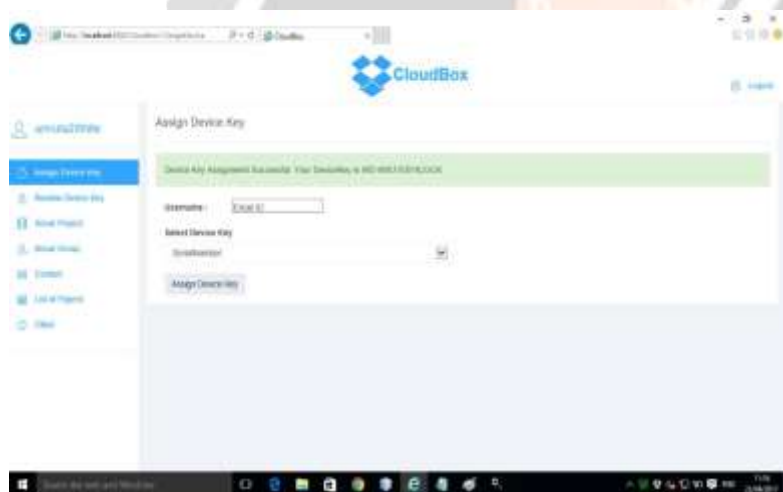
[5]



[6]



[7]



4. CONCLUSION

In this paper, we introduced data security protection mechanism for cloud storage system. In which a data sender is allowed to encrypt the data with the help of identity of receiver. And the receiver requires both secret key and security device to get access of data. Our aim is to enhance the confidentiality of the data and offer the revocability of the device. once the device is revoked then SDAM will offer new unique or personal security device to user.

5. REFERENCES

- [1] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Senior Member, IEEE “Two-Factor Data Security Protection Mechanism for Cloud Storage System”, *TRANSACTIONS ON COMPUTERS*, VOL. 65, NO. 6, JUNE 2016.
- [2] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 468–477, Feb. 2014.
- [3] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C. Hu, “Dynamic audit services for outsourced storages in clouds,” *IEEE Trans. Services Comput.*, vol. 6, no. 2, pp. 227–238, Apr.–Jun. 2013.
- [4] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, “DAC-MACS: Effective data access control for multiauthority cloud storage systems,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1790–1801, Nov. 2013.
- [5] F. Zhao, T. Nishide, K. Sakurai. “Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control”. *Information Security and Cryptology, LNCS*, pp.406-418, 2012.
- [6] Q. Tang, P. H. Hartel, and W. Jonker, “Inter-domain identitybased proxy re-encryption,” in *Information Security and Cryptology. Berlin, Germany: Springer-Verlag*, 2008, pp. 332–347.
- [7] D. Boneh, C. Gentry, B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys”, *Advances in CryptologyCCrypto 2005*, pp.258-275, 2005.
- [8] B. Waters introduced, “Efficient identity-based encryption without random oracles,” in *Proc. 24th Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2005, pp. 114–127.

