www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 2, Issue – 4. April 2016

Data Accessing Priority from Cloud Storage Using Attribute Based Encryption

A.Silambarasan[#1], R.Varatharajan[#2], T.Anitha Devi[#3]
Department of Information technology
Karpaga Vinayaga College of Engineering and Technology
Kanchipuram, Tamil Nadu, India
[1]silambarasanstr77, [2]ravivaratharajan, [3]t.anithadevicse @gmail.com

***Abstract*---Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Attribute-based encryption is used in various schemes proposed to secure the cloud storage. Here the project existing work is achieving AnonyControl for semi anonymous process not only the data privacy content also user identity details leakage. We are proposing system is to proper security user identity details to achieve the fully anonymous process AnonyControl-F. Firstly user identity details we needed proper authentication purpose. The data owner upload a files in cloud storage need to request for N Attribute-Authorities, then authority giving key for data owner for upload files. After upload a files cloud storage any of the people going to see files the file is fully encrypted format saved in allocated Drive. Also support only Disjunctive Normal Form (DNF) is a standardization (normalization) Boolean logic encryption policy. The proposed schemes are able to protect user's privacy against each single authority. The data consumer downloads at a time notification message from data owner. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. We provide detailed analysis on security performance to show feasibility of the scheme AnonyControl and AnonyControl-F. This project we are produced AnonyControl and AnonyControl-F security analysis provides encryption and decryption based on bilinear Diffie-Hellman assumption, and the feasibility our schemes exhibits evaluation performance.**

***Index terms*---Cloud computing, Secured data accessing.**

I. INTRODUCTION

Cloud computing is a revolutionary based computing paradigm, which enables flexible, on demand, and low cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. This system does not achieve the fully anonymous process and secure the data partially achieve. The identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). Preferably, any authority or server alone should not know any client's personal information. The users in the same system must have their private keys re-issued so as to gain access to the re-

encrypted files, and this process causes considerable problems in implementation. In existing system, at the time of file downloaded by the consumer file notification is not sent to data owner. In my project, on that time notification related to that file is sent to data owner. In existing system upload the files to cloud storage, the cloud server and N Attribute-Authorities view the uploaded files but in my project, uploaded files are not visible to cloud server and N Attribute-Authorities. Here, data owner wants key to upload the files that key is given by N-Authorities by requesting for the key. The key is sent to mail id.

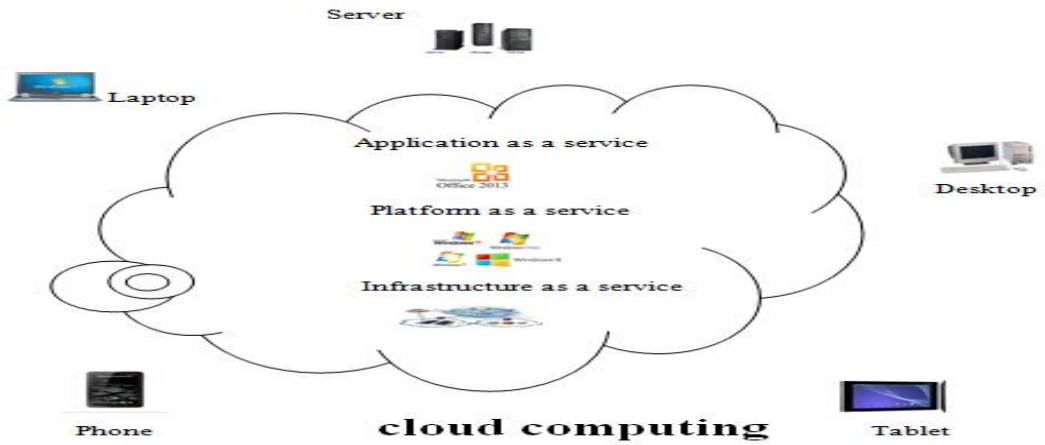

Fig.1: Services provided in cloud computing

II. LITERATURE SURVEY

The researcher V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, done by restricted number of consumers only accessing data, in this proposed project N-number of consumers accessing the data.

The researcher A. Sahai and B. Waters, in Advances in Cryptology. Berlin, Germany: Springer-Verlag. In this fuzzy identity based encryption means (set of instuction)user id is not fully anonymous process and user data is visible to all then any unkown person can easily hacking our data. In this proposed system, we are going to do this by using fully anonymous - Attribute based encryption. By using this technique, we provide authenticated user identity.

The researcher C. Wang, Q. Wang, K. Ren, and W. Lou, done the securely introduce an effective TPA the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user.

III. PROPOSED SYSTEM

In various schemes of ABE like IBE, KP-ABE, CP-ABE also one access control system. but the common problem with this techniques is no authentication to user details. The data confidentiality, less

effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. We propose AnonyControl and AnonyControl-F allow cloud servers to control users' access privileges without knowing their identity information. In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. Considered the basic threshold-based Key Policy -Attribute Based Encryption (KP-ABE). Many attribute based encryption schemes having multiple authorities have been proposed afterwards. In our system, there are four types of entities: N Attribute Authorities (denoted as *A*), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N is joint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

A. Advantages of Proposed System

The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The proposed schemes are tolerant against authority compromise, and compromising of up to $(N-2)$ authorities does not bring the whole system down. We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F. We firstly implement the real toolkit of a multiauthority based encryption scheme AnonyControl and AnonyControl-F.

IV. ARCHITECTURE DIAGRAM

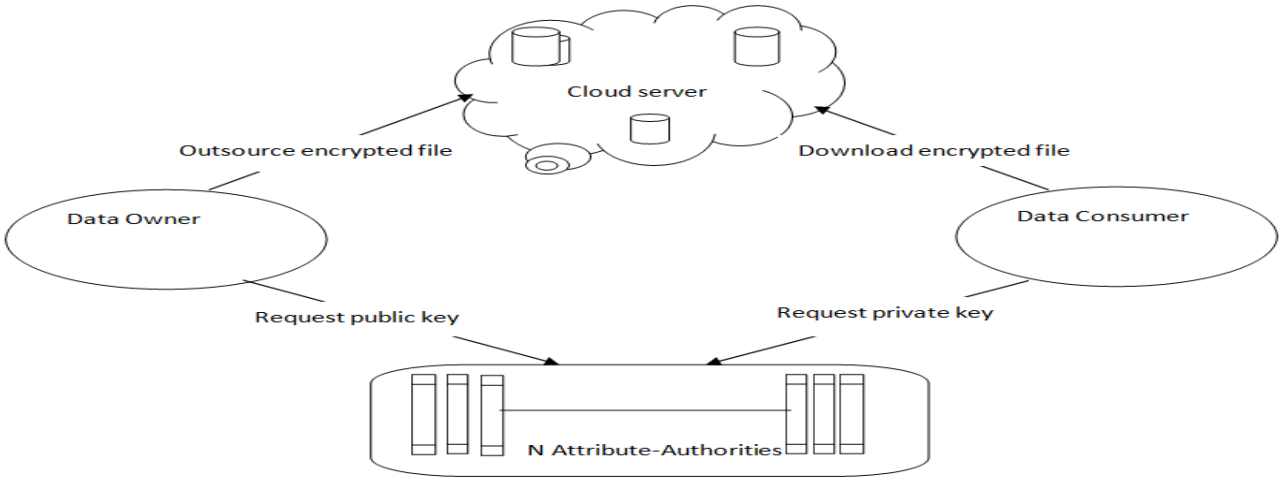

Fig.2: Overall Architecture of a system

V. METHODOLOGIES

The different modules are used to secure the user details and uploaded files. We are using the methodology called attribute based encryption. Through this technique, to upload a file in cloud storage data owner needs a key. That key will be got by requesting the key to the N-authorities. After the key is provided to the data owner then the file is uploaded as encrypted file and it is visible to data owner only. Consumer who wants the file also should know the key to access the file. Here we are using another methodology called decisional bilinear Diffie-Hellman method for encryption of data being uploaded.

VI. MODULE DESCRIPTION

A. Registration Based Social Authentication

Initially we are doing registration module to authentication purpose for user details. User registered their details at that time automatically unique password is sent to his mail. The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few(e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's Registration.

B. Security Module

In security module, we are going to provide the unique details for authentication purpose. Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. Trustee based social authentication systems ask users to select their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees.

C. Attribute Based Encryption Module

In attribute based encryption data owner file should be changed in encrypted files. Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. the attribute-based encryption have been proposed to secure the cloud storage. Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a Decryptor's identity has some overlaps with the one specified in the ciphertext.

D. Multi-Authority Module

A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

VII. FUTURE ENHANCEMENT

In future by sending the keys to the mobile to increase the security to the file and user details and also by using the biometric devices to accessing the files more secure and effectively. Direction for future work is to allow multi authority servers to update user secret key without disclosing user attribute information.

VIII. CONCLUSION

Finally, we are doing the project using attribute based encryption to secure the files and user details that are uploaded in the cloud. Through this technique, to upload a file in cloud storage data owner needs a key. That key will be getting by requesting the key to the N-authorities. After the key is provided to the data owner then the file is uploaded then the file is uploaded as encrypted file and it is visible to data owner only. Consumer who wants the file also should know the key to access the key. Here we are providing the authentication to the user details.

REFERENCES

[1]. Taeho Jung, Xiang-Yang Li, *Senior Member, IEEE,* Zhiguo Wan, and Meng Wan, *Member, IEEE*,"**Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption**", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015.

[2]. V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "**Multi-authority attribute-based encryption with honest-but-curious central authority,**" *Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.*

A. Sahai and B. Waters, "**Fuzzy identity-based encryption**," in *Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.*

[3]. C. Wang, Q. Wang, K. Ren, and W. Lou, "**Privacy-preserving public auditing for data storage security in cloud computing,**" in *Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.*

[4]. S. Müller, S. Katzenbeisser, and C. Eckert, "**On multi-authority ciphertext-policy attribute-based encryption**," *Bull. Korean Math. Soc.*, vol. 46, no. 4, pp. 803–819, 2009.