Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 3, March 2017, pg.204 – 211

Secure and Authorised De-Duplication

Nancy P
Associate Professor, Rajalakshmi Engineering College
nancy.p.11.cse@rajalakshmi.edu.in

Raveena Pooja K
Student, Rajalakshmi Engineering College
pooja.kankeyan@gmail.com

Priyadharshini R
Student, Rajalakshmi Engineering College
priyapd.menon@gmail.com

Ramya R
Student, Rajalakshmi Engineering College
ramyaradha96@gmail.com

Abstract— Our technique uses an advanced duplication system supporting authorized duplicate check and compares the storage system with file content. In this new duplication system, the private keys will not be issued to users directly, which will be kept and managed by the private cloud server instead. In this way, the users cannot upload the same hash value data because it compares the whole data base storage system, which means that it can prevent the duplication process with same content.

Keywords— File Upload/Download, Secure Key, Encryption.

I. INTRODUCTION

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine- grained data access control is desired.

The problem of simultaneously achieving scalability and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and

enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine- grained data access control to untrusted cloud servers without disclosing the underlying data contents. Present system achieves this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE) and Advanced Encryption Standard (AES). Present System shows secure ABE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Convergent encryption, to support duplicate check, the key is derived from the file *F* by using some cryptographic hash function. The main purpose is to protect the data security by including differential privileges of users in the duplicate check. The main idea of our technique is that the novel encryption key generation algorithm. For simplicity, we will use the hash functions to define the key generation functions and convergent keys

II. LITERATURE SURVEY

- Chun-1 Fan solve the issues if an encrypt or can ensure that only the receivers who match the restrictions on predefined attribute values associated with the ciphertext can decrypt the ciphertext.
- Kan Yangand proposed a design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently.
- JinLi deals proposed a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. Author's new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally.
- Eric Zavattoni proposed the design of a software cryptographic library that achieves record timings for the computation of a 126-bit security level attribute-based encryption scheme. We developed all the required auxiliary building blocks and compared the computational weight that each of them adds to the overall performance of this protocol.
- YanZhu proposed a practical cryptographic RBAC model, called role-key hierarchy model, to support various security features, including signature, identification, and encryption on role-key hierarchy.
- The work proposed by Bharti Ratan Madnani deals with exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Key Policy Attribute-Based Encryption, Proxy Re-Encryption (PRE) algorithm are used in the proposed scheme has salient properties of user access privilege confidentiality and user secret key accountability.

- Sushmita proposed DACC (Distributed Access Control in Clouds) algorithm, where one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records. Thus, a single key replaces separate keys from owners. Owners and users are assigned certain set of attributes. Owner encrypts the data with the attributes it has and stores them in the cloud. The users with matching set of attributes can retrieve the data from the cloud.

III. ADVANCED ENCRYPTION ALGORITHM

The technology used in this system is AES (Advanced Encryption Standards), with the symmetric key encryption. In the proposed system, Two Layered Encryption is done to maintain the data secured, data owner performs a coarse-grained encryption, and in the cloud which performs a fine-grained encryption on top of the owner encrypted data. The challenging issue is how to purify Access Control Policies (ACPs) such that the two layer encryption can be performed. This system shows that these problems is NP-complete and propose new optimization algorithms. This system utilizes an efficient group key management scheme that supports expressive ACPs. This system assures the secrecy of the data and preserves the privacy of users from the cloud server while entrusting most of the access control enforcement to the cloud servers.

IV. ADVANCED SEARCH

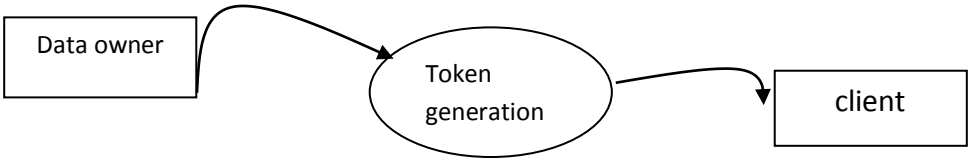
The problem of integrity auditing and secure deduplication on cloud data. Specifically, aiming at achieving both data integrity and deduplication in cloud. To avoid repeated full backups of the same file system and backups of files that happen to reside in multiple places. For this process, we have followed the following steps,

- System Initialization: This module consists of certificate authority(CA) and attributes authorities (AAs),setup with the proposed system. The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the social security administration, an independent agency of the united states government. Each user will be issued a social security number(SSN) as its global identity. Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain.
- Secret Key Generation by AAs: The secret key generation algorithm is run by each AA. In this scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes. Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.
- Data Encryption by User: Owner first encrypt the data m with content keys by using symmetric encryption methods, and then they encrypt the content keys by running the encryption algorithm: Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption

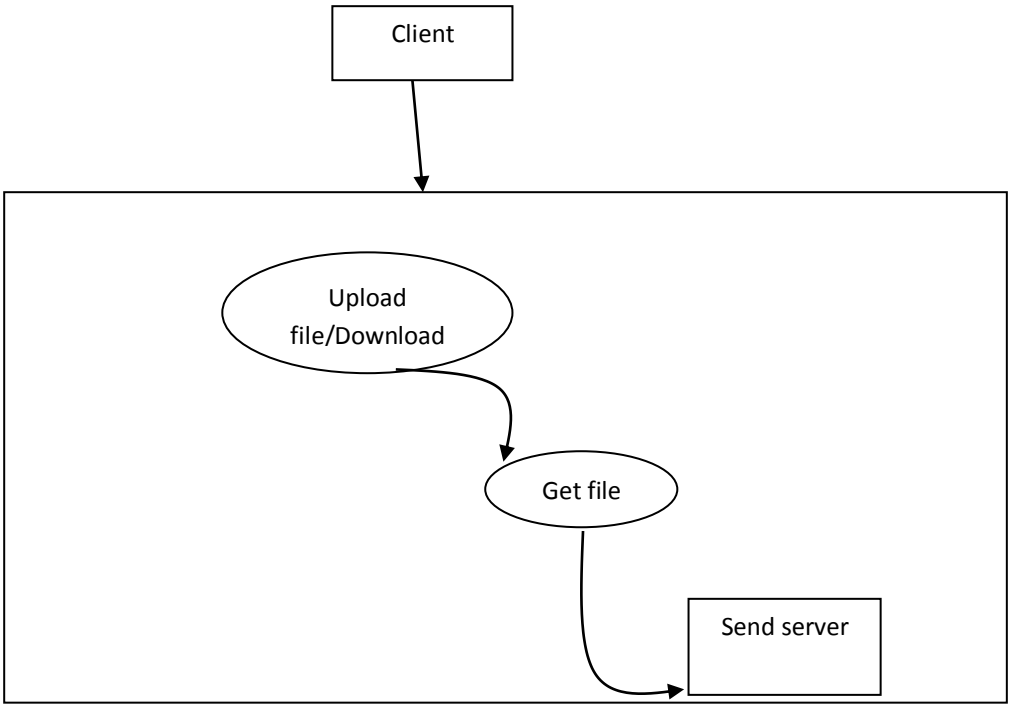
techniques (AES).Then the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies. It divides the data into several data components as m = (m_1….m_n) according to the logic granularities. For example, the personal data may be divided into {name,address,securitynumber,employer,salary}.It encrypts data components with different content keys k = (k_1…k_n) by using symmetric encryption methods (AES).It then defines an access structure Mi for content key Ki=(i…n) and encrypts it by running the encryption algorithm encrypt.

V. DFD

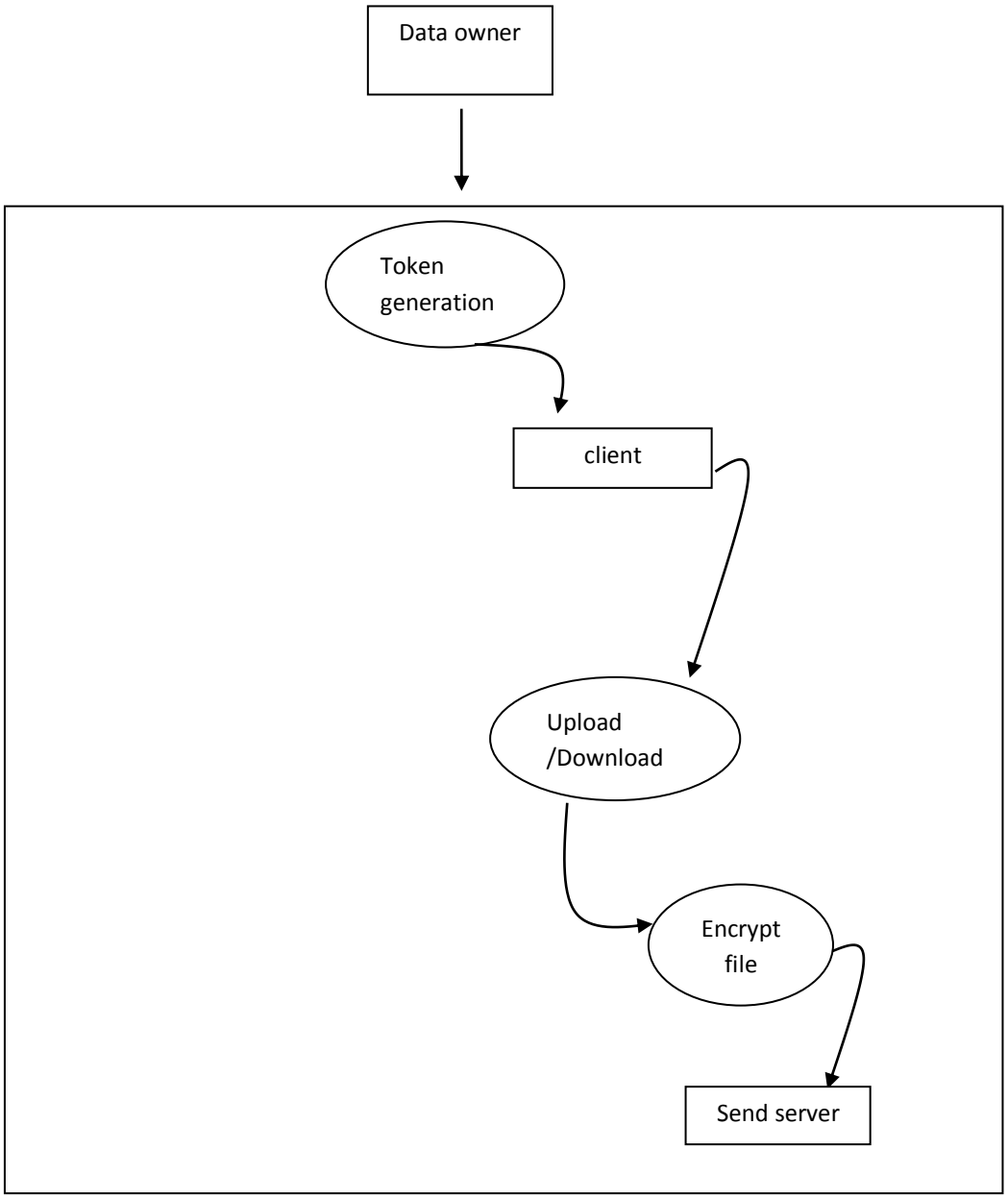
I.



II.

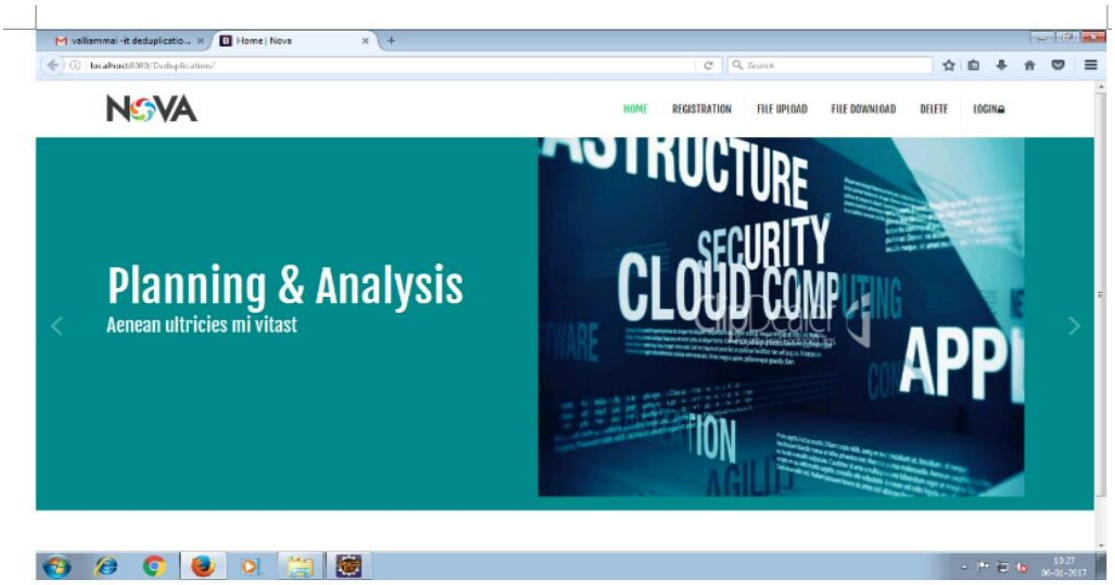


III.

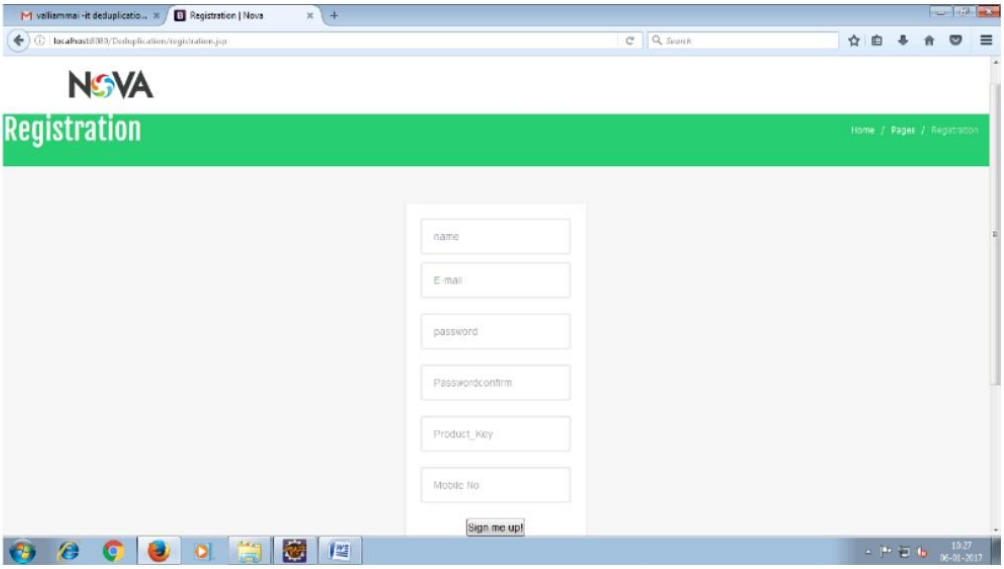


VI. WORKING SCREENSHOTS

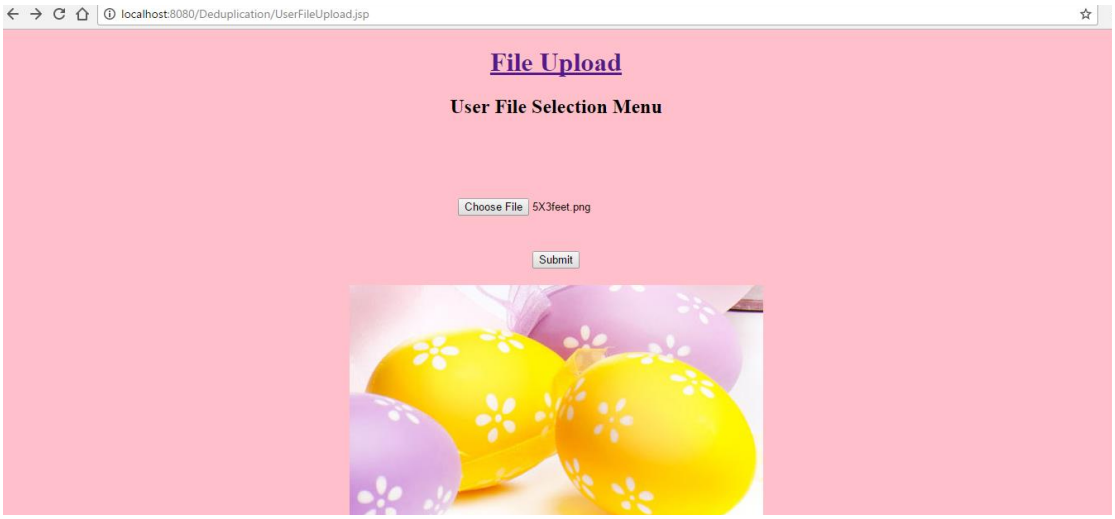
I.



II.



III.



IV.

VII. FUTURE WORKS

Based on the proposed AES scheme, develop a secure cloud data storage architecture using a hybrid cloud infrastructure. This hybrid cloud architecture is combination of public and private cloud in real time data centres cloud storage system.

VIII. CONCLUSION

The proposed system present system achieves goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE) and Advanced Encryption Standard (AES).Present System shows secure ABE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. In ABE, data are associated with attributes for each of which a public key component is defined. The encrypted associates the set of attributes to the message by encrypting it with the corresponding public key components. Based on the proposed ABE scheme, develop a secure cloud data storage architecture using a hybrid cloud infrastructure. This hybrid cloud architecture is a composite of private cloud and public cloud, where the private cloud is used to store only the organisation's sensitive

structure information such as the role hierarchy and user membership information, and the public cloud is used to store the actual data that is in the encrypted form.

REFERENCES

[1] Arbitrary-State Attribute-Based Encryption with Dynamic Membership by Chun-I Fan, , Vincent Shi-Ming Huang, and He-Ming Ruan - IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 8, AUGUST 2014.
[2] Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage by Kan Yangand Xiaohua Jia, Fellow - IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 7, JULY 2014
[3] Securely Outsourcing Attribute-Based Encryption with Check ability by Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang - IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 8, AUGUST 2014
[4] Software Implementation of an Attribute-Based Encryption Scheme by Eric Zavattoni,Luis J,Dominguez Perez,Shigeo Mitsunari-IEEE,FEBRUARY 2014.
[5] Role-Based Cryptosystem: A New Cryptographic RBAC System Based on Role-Key Hierarchy by Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Di Ma, and Shanbiao Wang- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12, DECEMBER 2013
[6] Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation by Bharti Ratan Madnani, Sreedevi - International Journal of Innovative Research in Computer and Communication Engineering *Vol. 1, Issue 3, May 2013*
[7] Cryptographic Roles in the Age of Wikileaks by Mikko Kiviharju,Riihimaki,Finland-IEEE Military communications conference,2013
[8] From RBAC to ABAC:Constructing Flexible Data Access Control for Cloud Storage Services by Yan Zhu,Dijiang Huang-IEEE TRANSACTION ON SERVICES COMPUTING 2013.

