INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2945 - 2952
RECEIVED : 25.02.2018 PUBLISHED : 27.03.2018
March 27, 2018

Cloud Integrating Dual System Encryption Technology with Selective Proof Technique for Mobile

M. D. Dinesh[1], M. Jayachandran[2], U. Moulishankar[3], P. Latha M.E[4]
Department of Computer Science and Engineering
Students[1,2,3], Assistant professor[4]
Kingston Engineering College, Vellore, Tamil Nadu, India.

Abstract
This paper, proposes a new secure data sharing scheme for Mobile Computing as an enhancement to A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing Model by integrating the dual system encryption technology with selective proof technique. While the introduced scheme supporting any standard access structures is built in the composite structure bilinear group, it is verified adaptively CCA secure in the standard technique without threatening the expressiveness of access policy. In this paper, we attempt in addition to make an enhancement for the model to obtain more efficiency in the re-encryption key generation and re-encryption phases. Proxy Re-Encryption (PRE) is an effective cryptographic essential model that permits a data owner to nominee the access rights of the encrypted data which are stored on a cloud storage system to remaining entities without leaking the information of the data to the honest-but-curious cloud server. It implements the effectiveness for data sharing's the data owner even working with limited resource devices (e.g. mobile devices)can offload most of the computational activity to the cloud. Since its establishment many variants of PRE have been recommended and proposed. A Cipher text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE), which is observed as a regular approach for PRE, engages the PRE technology in the attribute-based encryption cryptographic frame work as like that the proxy is granted to make change an encryption down an access policy to another encryption under a new access policy. CP-ABPRE is suitable to numerous real time network appliances, like sharing secure data in the mobile cloud applications.

Keywords: Mobile Computing**;** Proxy Re-Encryption**;** data sharing**;** mobile devices

1. INTRODUCTION

Evolution of cloud computing started during the year 1950's with the concept of a mainframe computer. Mainframe consists of multiple users who have the ability to access central computers. The mainframe is capable of storing larger data and Processing too. The main disadvantage is that the cost of buying a mainframe computer is high and difficult to maintain the overall systems. After that, in 1970's virtualization technique has been introduced. It is the main reason for the empowerment of the cloud computing. Fig. 1 shows that various virtual machines with software are working under a different platform. Machines allow simultaneous operation for more than an operating system; furthermore, it provides the same processing to the numerous interconnected computers, as well it has an ability to reside the entire computing environments into one physical environment. In 1960's ARPANET was developed.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2945 - 2952
RECEIVED : 25.02.2018 PUBLISHED : 27.03.2018
March 27, 2018

According to the large-scale organization, this was one of the first public networks, which allowed computers to access data from anywhere. To overcome all those above-mentioned issues, Distributed computing [2] has been introduced

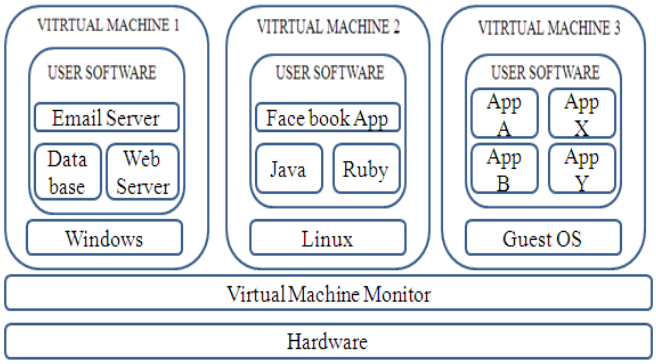

Fig. 1. Hardware virtualized server hosting
Three virtual machines

Distributed computing are the collections of grid computing and utility computing. it shares the compute and storage resources distributed across different administrative domains.

The open grid services' architecture addresses this need for standardization grid systems. Global toolkit is a middleware that implements many standard grid services, and over the years has aided the deployment of a number of service-oriented grid infrastructure and applications. Which facilitate user interaction with multiple middleware's and implements policies to meet QoS needs. Utility computing and grid computing having many issues, initially grid resources management technique did not ensure fair and equitable access to resources in many systems. Traditional metrics failed to capture the more subtle requirement of users. There were no real incentives for users to be flexible about resource requirement or job deadlines in utility environment users assign a utility value to their jobs. Fig. 2 shows the overall evolution of cloud that is the combination of entire grid virtualization, grid and utility computing.

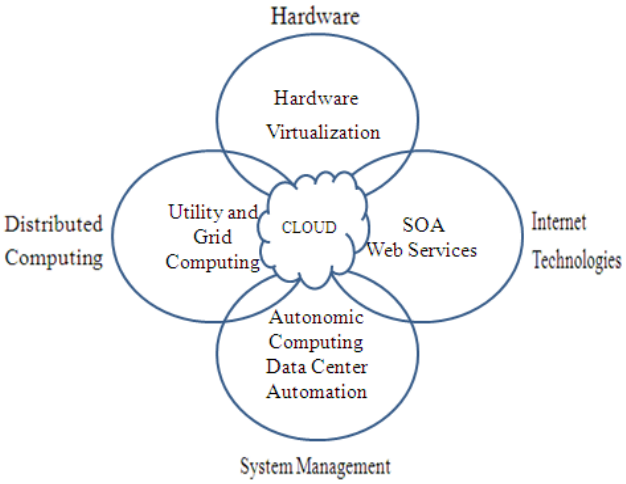

Fig. 2. Convergence of various advances
Leading to the advent of cloud computing

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2945 - 2952
RECEIVED : 25.02.2018 PUBLISHED : 27.03.2018
March 27, 2018

fig. 3 shows that the working based on three service models: PaaS, SaaS and IaaS. In software as a service model we have consumer activities and provider activities. The consumer uses applications for business process operation. Providers maintain manage and support the software application on cloud infrastructure. in platform as a service also we have consumer and provider activity. Testing the application and managing the application will happen in consumer side providers provide deployment and administration tool to platform consumer. IaaS infrastructure as a service is fully based on infrastructure so it manages all the storage and networking process for IaaS consumers

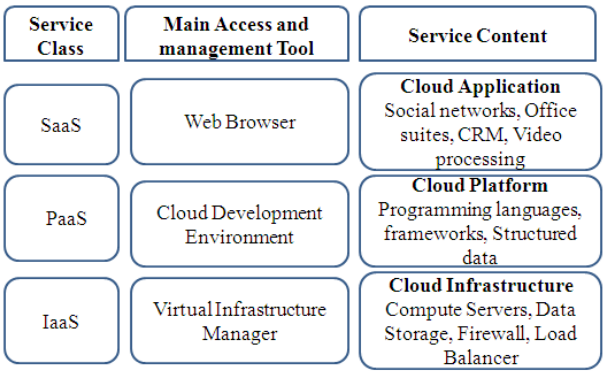

Fig. 3. The Cloud Computing Stack

Public cloud [3] is the open use to the public by a particular organization. It is hosted, operated, and managed by a third-party vendor from one or more data canters. The service is offered to multiple customers. Private cloud differs from public clouds in that the network, computing, but it does not share with any other organization. Community, it supports several organizations that have externally hosted. Hybrid cloud includes two or more clouds, i.e., public and private. With a hybrid cloud, an organization might run the non-core application in a public cloud, while maintaining core application and sensitive data in-house in a private cloud.

After analyzing the Evolution of cloud computing, it is necessary that we need to find out what are all issues over a cloud storage system [1]. With the event of cloud computing and therefore the popularity of sensible mobile devices, individuals area unit bit by bit getting aware of a brand new era of knowledge sharing model in which the information is hold on on the cloud and therefore the mobile devices are accustomed store/retrieve the information from the cloud [11]. Typically, mobile devices solely have restricted cupboard space and computing power. On the contrary, the cloud has monumental amount of resources. In such a state of affairs, to realize the satisfactory performance, it's essential to use the resources provided by the cloud service supplier (CSP) to store and share the information. Nowadays, numerous cloud mobile applications have been wide used. In these applications, individuals (data owners) will transfer their photos, videos, documents and other files to the cloud and share these information with different people (data users) they wish to share.

CSPs conjointly give data management practicality for information homeowners. Since personal information files area unit sensitive, information home owners area unit allowed to choose whether or not to form their information files public or will only be shared with specific information users. Clearly, data privacy of the private sensitive information may be a huge concern for many information homeowners.

The progressive privilege management/access control mechanisms provided by the CSP area unit either not sufficient or not terribly convenient. They can't meet all the requirements of knowledge homeowners. First, once individuals transfer their information files onto the cloud, they're going the information in a place wherever is out of their management, and therefore the CSP could spy on user information for its business interests and/or different reasons. Second, individuals need to send Arcanum to every data user if they solely wish to share the encrypted information with sure users that is incredibly cumbersome. To modify the privilege management, {the information the info the information} owner will divide data users into totally different teams and send Arcanum to the groups that they require to share the information. However, this approach needs fine-grained access management. In both cases, Arcanum management may be a huge issue. Apparently, to resolve the on top of issues, personal sensitive information ought to be encrypted before uploaded onto the cloud in order that the information is secure against the CSP.

To address this issue [12], during this paper, we have a tendency to propose a Lightweight information Sharing theme (LDSS) for mobile cloud computing setting. The main contributions of LDSS area unit as follows:

We have a tendency to style associate degree rule known as LDSS-CP-ABE based on Attribute-Based cryptography (ABE) technique to offer economical access management over ciphertext.

We have a tendency to use proxy servers for cryptography and decryption operations. In our approach, machine intensive operations in ABE area unit conducted on proxy servers that greatly scale back the machine overhead on consumer facet mobile devices. Meanwhile, in LDSS-CPABE, in order to take care of information privacy, a version attribute is also other to the access structure. The coding key format is changed in order that it will be sent to the proxy servers during a secure means.

We have a tendency to introduce lazy re-encryption and outline field of attributes to scale back the revocation overhead once dealing with the user revocation downside.

Finally we have a tendency to implement an information sharing epitome framework supported LDSS. The experiments show that LDSS will greatly scale back the overhead on the consumer facet, which solely introduces a lowest extra price on the server facet. Such associate degree approach is useful to implement a realistic information sharing security theme on mobile devices. The results conjointly show that LDSS has higher performance compared to the prevailing ABE based mostly access control schemes over ciphertext.

2. LITERATURE SURVEY

J. Wei [4] proposed the Technique of proxy re-encryption, existing problem is that, solution is not scalable; In addition, a secure channel is essential for the key authority and for transmitting new keys by non-revoked users. So it requires the key authority to perform linear work in the number of non-revoked users the revocable identity-based encryption (RIBE) will be effective approach to fulfill the security requirements for data sharing.

J. Hong [5] says that, the basic algorithm and cryptography techniques to embed both time and attribute factors into access control for public cloud. Integrating attribute based encryption in public cloud storage leads an efficient scheme for secure fine grained access control. Disadvantage is that, it supports only the fine grained access control for time sensitive control.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2945 - 2952
RECEIVED : 25.02.2018 PUBLISHED : 27.03.2018
March 27, 2018

Ruixuan [6] author proposed an access control technology for normal cloud environment. Multiple revocation operations are incorporate into one, reducing the overhead. Compare to data files, the storage overhead needed for access control is very small In LDSS.

K. Fan [7] presents a lot of systematic, versatile and economical access management theme. The analysis results show the high potency of our theme. The standard access management strategy cannot effectively solve the safety issues that exist in knowledge sharing. This theme doesn't take into account the revocation of access permissions.

R. Jiang [8] proposed the Threshold multi-authority cipher text-policy (CP) ABE Access control scheme (TMACS). It satisfies the scenario of attributes from different AAs It can achieve security and system level robustness. Reusing of the master key shared among multiple attribute authorities (AAs). Security vulnerability, Data confidentiality, Personal information defined by each user's attributes set is at risk Resilient in security breach.

3. PROBLEM DEFINITION

All things considered, we can parcel these approaches into four arrangements: fundamental cipher text get the chance to control, different leveled get the opportunity to control, get the chance to control in light of totally homomorphic encryption and access control in perspective of trademark based encryption (ABE). Each one of these recommendation are expected for non-adaptable cloud condition. [9] Considered a specific conveyed figuring condition where data are gotten to by resource constrained phones, and proposed novel acclimations to ABE, which selected the higher computational overhead of cryptographic exercises to the cloud provider and cut down the total correspondence cost for the convenient customer[10].

4. PROPOSED SYSTEM

This paper, proposes another ensured data sharing arrangement for Mobile Computing as a move up to A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing Model by planning the twofold structure encryption development with particular confirmation technique. While the introduced plot supporting any standard access structures is worked in the composite structure bilinear social affair, it is checked adaptively CCA secure in the standard framework without undermining the expressiveness of access approach. In this paper, we try despite make an overhaul for the model to get greater profitability in the re-encryption key age and re-encryption stages.

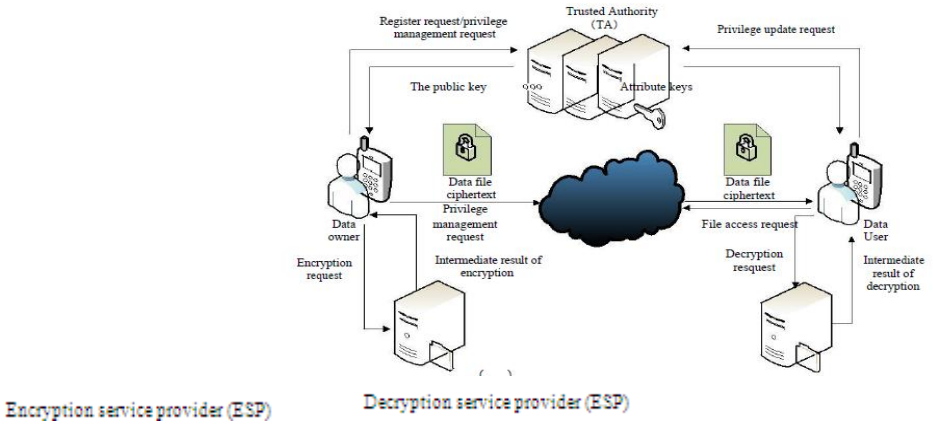

Fig. 4. A lightweight data-sharing scheme (LDSS) framework.

Fig. 4 illustrates that Data owner must register to access all the services that are provided by the cloud. Then using registration norms, data owner is easily registered within the few steps and by logging it through the data owner list. This diagram represents the data owner and data user transaction method with light weight deriving scheme like proxy re encryption and attribute based encryption method. Using this encryption method, data owner can easily able to upload the file to cloud with encrypted format. And based on the trusted authority access, attribute key is generated based on the key matching through the ESP. Date user must be register to process the data stored in the cloud that are provided by the data owner. If both the ESP and DSP verified the key value then there is no restriction to access the file through the cloud. Finally using the DSP, the uploaded file can be easily downloaded from the cloud.

5. SYSTEM MODEL

To better illustrate LDSS-CP-ABE algorithm, we first define the following terms.

Definition 1: Attribute

An attribute defines the access privilege for certain Data file. Attributes are assigned to data users by data owners. A data user can have multiple attributes corresponding to multiple data files. A data owner can define a set of attributes for its data files. The data accesses are managed by access control policy specified by data owners.

Let A = {A1, A2, A3... An} be the set of attributes for a Data owner. Each data user u also has a set of attributes Au, which is a non-empty subset of A, namely {A1, A2, A3... An}.

For example, assume A is {*relatives, colleagues, classmates, friends, teachers, peers, Hubei, Beijing, Shanghai, degree of intimacy*}. A data user's subset Au could be {*friend, Hubei, degree of intimacy=3*}. The access control policy for data file M could be: ((friends *and degree of intimacy > 1 and Hubei) or* (relatives *and peers)*), which means a data user cannot access M unless these conditions are met.

Definition 2: Access Control Tree

Access control tree is the specific expression of access control policies, in which the leaf nodes are attributes, and non-leaf nodes are relational operators such as *and*, *or*, *n of m threshold*. Each node in an access control tree represents a secret, and the secret of a top node can be split into multiple secrets by secret sharing scheme and distribute to lower level nodes. Correspondingly, if we know the secrets of leaf nodes, we can deduce the calculation recursively from bottom to top by the secret of non-leaf nodes.

Definition 3: Version Attribute.

Version attribute is introduced in LDSS-CP-ABE algorithm to ensure security. It is an addition to the original access control tree, forming a new root node of *and*. We have the following definitions.

T: The new access tree with version attributes.

S: The secret related to the root of T.

Ta, Ra, Sa: Ta is the initial access control tree and the left subtree of T. Ra is the root of Ta. Sa is the secret related to Ra.

Tv, Rv, Sv: Tv is the right subtree of T and contains only one node, which represents the version attribute Rv. Sv is the secret related to Rv.

Both Sa and Sv are derived from S based on the secret sharing scheme. For the example described in Definition 1, the access control tree with version attributes. LDSS-CP-ABE algorithm is designed using above Definitions. It includes four sub-functions:

Setup(*A, V*): Generate the master key MK, the public key PK based on attribute set A of the Data Owner and the version attribute V.

KeyGen(*Au, MK*): Generate attribute keys *SK*u for a data User *U* based on his attribute set *A*u and the master key *MK*.

Encryption(*K, PK, T*): Generate the cipher text *CT* based on the symmetric key *K*, public key *PK* and access control tree *T*.

Decryption(*CT, T, SK*u): Decrypt the cipher text *CT* using
the access control tree *T* and the attribute keys *SK*u . We explain all of these functions specifically below. First, function Setup() is called by the trusted third party (TA) to generate the master key and the public key. The master key is used to generate attribute keys and the public key is used to encrypt data files. The process of this function is given in Function 1.

CONCLUSION

In recent years, several studies on access management in cloud square measure supported attribute-based coding algorithmic program (ABE). However, ancient ABE isn't appropriate for mobile cloud as a result of its computationally intensive and mobile devices solely have restricted resources. During this paper, we tend to propose LDSS to handle this issue. It introduces a completely unique LDSS-CP-ABE algorithmic program to migrate major computation overhead from mobile devices onto proxy servers, so it will solve the secure information sharing drawback in mobile cloud. The experimental results show that LDSS will guarantee information privacy in mobile cloud and cut back the overhead on users' facet in mobile cloud. Within the future work, we'll style new approaches to make sure information integrity. To additional faucet the potential of mobile cloud, we'll conjointly study the way to do ciphertext retrieval over existing information sharing schemes.

REFERENCES

[1] S. Singh, Y.S. Jeong, J.H. Park, "A survey on cloud computing security: Issues, threats, and solutions," Journal of Network and Computer Applications, pp. 200-22, Nov 2016.

[2] A. Agarwal, S. Siddharth, and P. Bansal. "Evolution of cloud computing and related security concerns," Symposium on Colossal Data Analysis and Networking, pp. 1-9, IEEE, 2016.

[3] Y. Ren, J. Xu1, J. Wang, and J.U Kim, "Designated-Verifier Provable Data Possession in Public Cloud Storage," International Journal of Security and Its Applications , Vol. 7, No. 6 , pp.11-20, 2013.

[4] J. Wei, W. Liu, X. Hu, " Secure data sharing in cloud computing using revocable-storage identity-based encryption," IEEE Transactions on Cloud Computing, 2016, Mar 23.

[5] J. Hong , K, Xue, Y, Xue, W, Chen, DS, Wei , N, Yu, P, Hong, "TAFC: Time and attribute factors combined access control for time-sensitive data in public cloud," IEEE Transactions on Services Computing, 2017 Mar 14.

[6] Li, Ruixuan, C. Shen, He, Heng, Z. Xu, and Cheng-Zhong Xu. "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," IEEE Transactions on Cloud Computing , 2017.

[7] K. Fan, Q. Tian, J. Wang, H. Li, and Y. Yang, " Privacy protection based access control scheme in cloud-based services," China Communications, 14(1), pp.61-71.

[8] X. Wu, R. Jiang, and B. Bhargava, "On the security of data access control for multiauthority cloud storage systems," IEEE Transactions on Services Computing, 10(2), pp.258-272, 2017.

[9] G. V. Kapse, V. M. Thakare, S. S. Sherekar, and A. V. Kapse," Multi-Authority Data Access Control For Cloud Storage System With Attribute-Based Encryption.

[10] Z. Mahmood, " Data location and security issues in cloud computing. In Emerging Intelligent Data and Web Technologies (EIDWT)," International Conference ", pp. 49-54, IEEE, 2011 September.

[11] C, Gentry, S, Halevi, "Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT," Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[12] Z. Brakerski, V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science," California, USA: IEEE press, pp. 97-106, Oct. 2011.