ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (96-100), Month: July - September 2015, Available at: www.researchpublish.com

Application Centric Cloud Infrastructure Based On Iaas with a Secure File System

Dr. M.N. Jayaram[1], Mahesh H N[2]

Associate Professor (Dept. of E&C) [1], PG Student (NIE) [2], S.J.C.E College of Engineering, Mysore, India

Abstract: **Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centres located throughout the world. In the present technologies, the cloud based application has a flexible, on demand computing infrastructure. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. Here by access control can provide the security in each layer of network, server and application. This survey paper aims to elaborate and analyze the numerous unresolved issues threatening the Cloud Computing. Our work will enable researchers and security professionals to know about user and vendor concerns and critical analysis about the different security models and tools proposed.**

Keywords**: Cloud Infrastructure, Access control, Attribute Based Encryption, Secure Cloud Computing.**

I. INTRODUCTION

Internet has been a driving force in today's various technologies that have been developed. One of the most used technology is cloud computing. Cloud computing is an application or service that runs on a distributed network using virtualized resources and accessed over internet. Cloud services allow individuals to use software and hardware that are managed by third parties at remote locations. Cloud services include online data storage, social networking sites, webmail, and online business applications. Cloud computing can significantly reduce the cost and complexity of the networks and other benefits to users include scalability, reliability, and efficiency [8].

There are four Deployment Models of Cloud Computing:

Private Cloud**:** A private cloud is used for particular organization that controls the virtualized resources. Example: SOX, HIPAA, SAS 70.

Public Cloud**:** Public clouds are used for general public use by a particular organization or company to offer access to computing resources at minimal cost. With public cloud services, users don't need to purchase software, hardware or supporting infrastructure. Example: Rackspace, Amazon Web Services (AWS), Microsoft Azure, Google App Engine [10].

Community Cloud**:** Shared through various organizations or company. Example, Google managed government cloud.

Hybrid Cloud**:** Hybrid cloud mean more than two cloud form a single cloud. It takes the advantages in scalability and cost effectiveness. Example: Amazon s3 [1].

This paper is organized as follows. Section II provides a Literature Survey. Section III describes the proposed method. In Section IV, experimental results of described techniques are shown. In the next section, the conclusion and future work are given.

II. LITERATURE SURVEY

Several works have been formulated for securing a file in cloud by using Attribute based encryption.

V. Goyal, O. Pandey[13] proposed that a more sensitive data is shared and stored on cloud by Internet, there will be a need to encrypt data stored at the cloud. One drawback of encrypting data is that it can be shared only at a giving your private key to another party. They develop a new cryptosystem for fine-grained sharing of encrypted data that call Key-

Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, encrypted data are labeled with sets of attributes and private keys are associated with access structures that control which data a user is able to decrypt but it is complex procedure. R. Ostrovsky, A. Sahai [5] constructs an Attribute-Based Encryption (ABE) scheme that allows a user's private key to be expressed in terms of any attributes. Previous ABE schemes were limited to expressing only monotonic access structures. They provide a proof of security for scheme Decisional Bilinear Diffie-Hellman (BDH) assumption. Furthermore, the performance of this new scheme compares favourably with existing, less-expressive schemes but not up to the mark .B. Waters present a new methodology to analyze Ciphertext-Policy Attribute Encryption (CP-ABE)[14]. This solution allows any data owner to specify access control in terms of any attributes in the system. In our most efficient system, ciphertext size, encryption, and decryption linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model . A. B. Lewko, T. Okamoto, K. Takashima present two fully secure functional encryption schemes: a fully secure attribute-based security scheme and a fully secure (attribute-hiding) predicate encryption (PE) scheme. In both cases, previous constructions were only proven to be selectively secure. Both results use novel strategies to adapt the dual system encryption methodology introduced by Waters construct new ABE scheme in Composite order bilinear groups, and prove its security for static assumptions. New ABE scheme supports monotone access formulas means one can access in any one type of attributes. Predicate encryption scheme is constructed via a new approach on bilinear pairing proposed by Okamoto and Takashima.

III. PROPOSED METHOD

In this paper, We first modify the original model of ABE with outsourced decryption in existing system to allow for verifiability of the transformations. After describing the formal definition of verifiability, we propose a new ABE model and based on this new model construct a concrete ABE scheme with verifiable outsourced decryption. Our scheme does not rely on random oracles.

Advantages of Proposed System:

- In proposed scheme cannot not use same password for more than once.
- Proposed scheme does not rely on random oracles.
- The scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.
- Decryption is not an expensive.
- Data owner has no worry for data credentials.

Existing System of a Secure File System:

- The authors Green and Wates *et al.* proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes or access policy into a simple ciphertext, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed ciphertext.

Disadvantages of Existing System:

- One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a ciphertext grows with the complexity of the access policy. At the cost of security, only proven in a weak model (i.e., selective security), there exist several expressive ABE schemes where the decryption algorithm only requires a constant number of pairing computations.

System Architecture:

- Large systems are always decomposed into sub-systems that provide some related set of services. The initial design process of identifying these sub-systems and establishing a framework for sub-system control and communication is called Architecture design and the output of this design process is a description of the software architecture.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (96-100), Month: July - September 2015, Available at: www.researchpublish.com

- The architectural design process is concerned with establishing a basic structural framework for a system shown in figure 1. It involves identifying the major components of the system and communications between these components

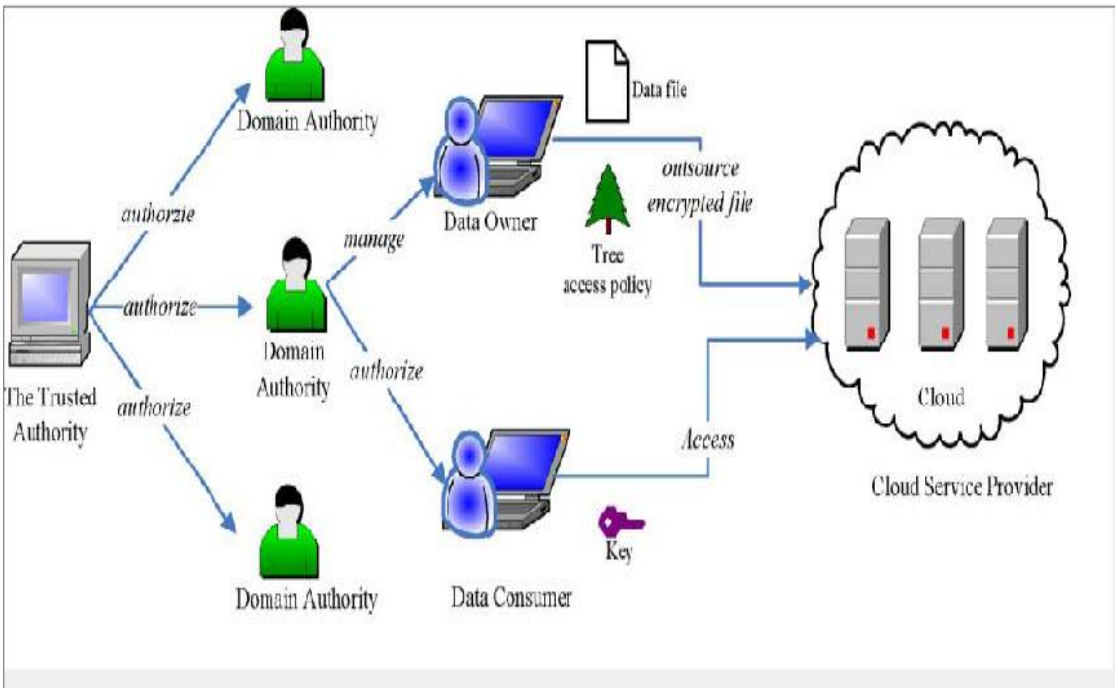

Figure 1: System Architecture

VI. SOFTWARE IMPLEMENTATION

A sequence diagram in Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Figure 2shows Sequence diagram that is sometimes called event diagrams, event scenarios, and timing diagrams.

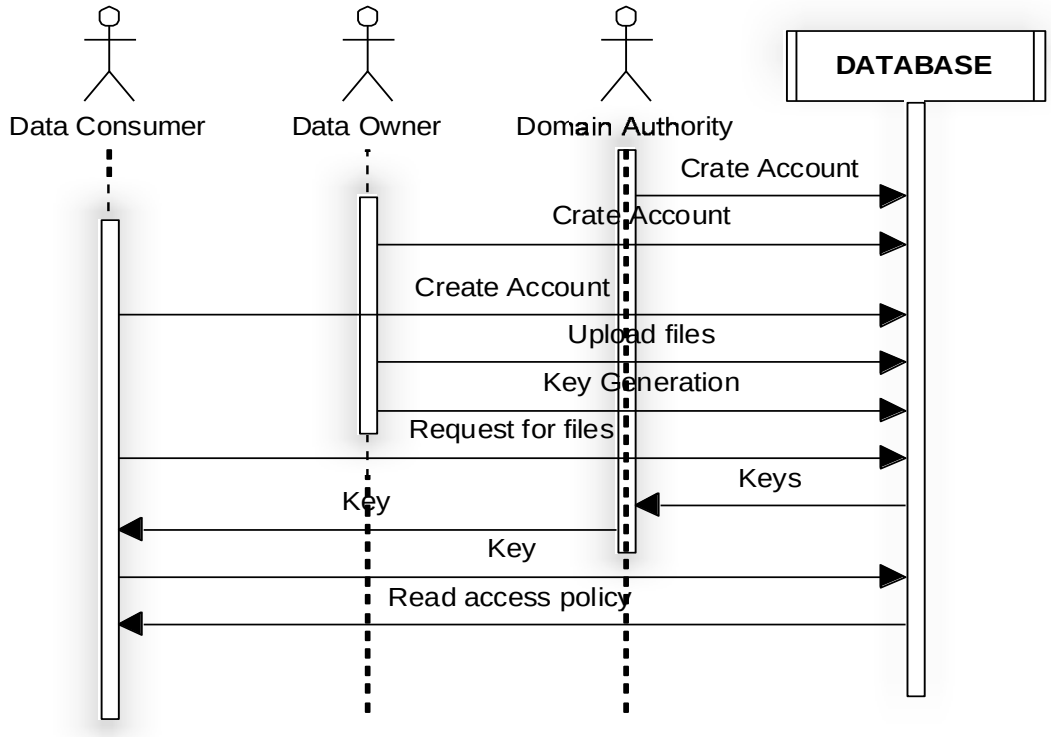

Figure 2: Sequence Diagram

Algorithm:

1) In this module, first develop the system module, which consists of cloud service provider who create a trusted domain authority or say manager. Then manager will register the Data Owner and data consumer.

Where manager give unique ID and password to each by which they can access to cloud through virtual networks.

2) When a new user wants to join the system, with the aid issues an attribute private key to him/her based on his/her attributes. Based on the system model provided attempt to define an underlying primitive with outsourced key-issuing and decryption for realizing our access control system.

3) In this module, we develop the file upload module process, where, when a data owner wants to outsource and share a file with some users, he/she encrypts the file to be uploaded under a specified attribute set (resp. access policy). Whenever a data owner wants to create and upload a file he/she firstly defines an attribute set (resp. access structure). When a data owner wants to create and upload a file it considers attribute set (such as file name and size) based on this it generate a public key and private key to share with consumers.

4) In this module, we create the file access module, when a user wants to access an outsourced file; he/she downloads ciphertext from Storage-cloud service provider (S-CSP) and decrypts it with the help of Decrypt- cloud service provider (D-CSP) by requesting a key from domain authority person.

5) This module has developed to search the required data based on the Authors name or file name, it helps to find the data easily in the N number of data lists at secured cloud.

6) When there is a user to be revoked, updates affected users' private keys with the help of CSP, while the affected ciphertexts having been stored on S-CSP will be updated as well. When we want any user to be revoke or delete then we can delete their account.

V. RESULT

In any system results of processing are communicated to the users and to other system through outputs. In results it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. The concept of attribute based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent about attributes. In a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

VI. CONCLUSION

In this paper, we considered a new requirement of ABE with outsourced decryption: verifiability. We modified the original model of ABE with outsourced decryption proposed by Green *et al.* [12] to include verifiability. We also proposed a concrete ABE scheme with verifiable outsourced decryption and proved that it is secure and verifiable. Our scheme does not rely on random oracles. To assess the practicability of our scheme, we implemented it and conducted experiments in a simulated outsourcing environment. As expected, the scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.

REFERENCES

[1] Cloud computing service composition: A systematic literature review Amin Jula, Elankovan Sundararajan, Zalinda Othman Expert Systems with Applications 41 (2014) 3809–3824

[2] Cloud Computing Security Requirements and Solutions: a Systematic Literature Review, Patrick Höner , University of Twente P.O. Box 217, 7500AE Enschede The Netherlands p.honer@student.utwente.nl

[3] Private Virtual Infrastructure: A Model for Trustworthy Utility Cloud Computing UMBC Computer Science Technical Report Number TR-CS-10-04

[4] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014, ISSN: 2277 128X

[5] Singh et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(6), June - 2013, pp. 1136-1142

[6] Asian research publication network Journals of Engineering and Applied Sciences. vol. 7, no. 5 May 2012 ISSN 1819-6608.

[7] International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013 2 ISSN 2250-3153

[8] Cloud computing service composition: A systematic literature review Amin Jula, Elankovan Sundararajan, Zalinda Othman Expert Systems with Applications 41 (2014) 3809–3824

[9] Private Virtual Infrastructure: A Model for Trustworthy Utility Cloud Computing UMBC Computer Science Technical Report Number TR-CS-10-04

[10] IOSR Journal of Computer Engineering (IOSRJCE) ISSN : 2278-0661 Volume 1, Issue 3 (May-June 2012), PP 28-36 www.iosrjournals.org

[11] 12023-cloud-computing-wp.pdf, dialogic, making innovations thrive.

[12] Cloud computing service composition: A systematic literature review Amin Jula, Elankovan Sundararajan, Zalinda Othman Expert Systems with Applications 41 (2014) 3809–3824

[13] Cloud Computing:Strategies for Cloud Computing Adoption Faith Shimba, Dublin Institute of Technology, faith.shimba@gmail.com, 2010-09-01

[14] Energy Efficiency for Data Center and Cloud Computing: A Literature Review, Volume 3, Issue 4, October 2013

[15] Literature review: Cloud Computing –Security Issues, Solution and Technologies, Rajani Sharma, Rajender Kumar Trivedi, Volume No.3, Issue No.4