ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

E-LEARNING SYSTEM WITH HIERARCHICAL ATTRIBUTE SET BASED ENCRYPTION ACCESS CONTROL IN CLOUD

M. Lawanya Shri*[1], M.B.Benjula Anbumalar[2], K. Santhi[3], Deepa.M[4]
[1]School of Information Technology and Engineering, Vellore Institute of Technology, Vellore-632014.
Email: kmlavanya@vit.ac.in

Received on 10-05-2016 *Accepted on 09-06-2016*

Abstract

Cloud Computing is a captivating computing archetypal where resources such as computing power, storage and software are provided as a service on the internet. Ease of provisioning, virtually infinite scalability and dynamism are some of key attributes of cloud computing. E-learning system is the significant technology trend, provides distribution and delivery of learning contents from different environments to the end users. In this paper we developed and implemented hierarchical attribute set based encryption access control technique through E-learning application and deployed in private cloud using open source technologies like Ubuntu Enterprise Cloud.

Keywords: E-learning System, Cloud Computing, Ubuntu Enterprise Cloud, VMware.

I. Introduction

Cloud computing is an emerging paradigm where many are shifting their data to cloud servers since it is cheaper for any individual or an enterprise to maintain its data without the actual money and human effort required to maintain their data in their own servers.

Cloud follows “pay-as-you-use” policy. The Traditional E-learning system is grounded on client/server architecture and they lack of flexibility, scalability, and interoperability. This brand the learning resources cannot be shared through diverse platforms. This application empowers learners to read materials and take examinations by themselves whenever they want.

Trainers provide materials and exercises in advance, and check results of learners at intervals.Cloud servers are commercial service providers and hence it is important to protect data on cloud servers from the CSPs and unauthorised accesses. This project provides fine-grained access control over the application that is only authorised users can have the access ability and the amount of data accessibility is also restricted according to a hierarchical structure. It also supports scalability and flexibility. This all in turn would increase the level of trust on data being stored on cloud servers among the users and hopefully number of users may increase.

II. Related Work

Key Policy Attribute Based Encryption: Shu cheng Yu, Cong Wang, Kui Ren, and Wenjing Lou et al discussed Key Policy Attribute Based Encryption scheme is a public key cryptography primitive that is for one-to-many communications. In this, data are associated with attributes for each of which a public key is defined [1][2]. The one who encrypts the data, i.e., the encryptor associates the set of attributes to the data or message by encrypting it with a public key.

Users are assigned with an access structure which is defined as an access tree over the data attributes. The nodes that are interior of the access tree are threshold gates and leaf nodes of the tree are associated with attributes. The secret key of the user is defined to reflect the access structure. So the user is able to decrypt the message that is a cipher text if and only if the data attributes satisfy the access structure. Expressive Key Policy Attribute Based Encryption-Neena Antony, A.

Alfred Raja Melvin et al discussed among the encryption methods in clouds. Attribute-based encryption (ABE)[13], allows adequate grained access control policy on the encrypted data. In the key policy Attribute based encryption, the primitive enables senders to encrypt the messages with a set of attributes and private keys in which are related with access tree structure that stipulates which all the cipher texts the key holder is allowed to decrypt. In most ABE systems, the size of the cipher text rises linearly with the number of cipher text attributes and the only known exceptions only support restricted forms of threshold access policies.

Cipher Text Policy Attribute Based Encryption-John Bethencourt, Amit Sahai, and Amit Sahai et al discussed that the user should retain certain set of credentials or attributes, so that the user can only able to access the data. In this paper the author proposed an enforcement policy to employ a trust worthy server to store the data and mediate specific access control policy [4]. Even if the storage server is not trust worthy, the data can be kept confidential by the encryption and decryption technique.

Hierarchical Identity Based Encryption- Neena Antony, A. Alfred Raja Melvin et al discussed the concept of HIBE technique gives detailed definitions of security. In this paper a two level HIBE concept consists of a root private key generator, domain private key generator , that are associated with PIDs that are arbitrary string length[5][6]. User retrieves private key from domain PKG which generates private key for their users.

III. Proposed Method

The main goal of this project is to develop a private cloud environment using Ubuntu Enterprise Cloud and also to develop an E-learning application. This application runs on the private cloud within an institution. The private cloud infrastructure is operated solely for that institution alone [6]. The infrastructure is managed either internally or by a third party. The proposed system involves building a private cloud infrastructure using Ubuntu Enterprise Cloud. The architecture of Ubuntu enterprise cloud consists of a frontend running with one or more Cloud Controller, Walrus, Cluster Controller, Storage Controllers with one or more nodes. The E-learning system is a web application developed using PHP. A user can access E-learning application from any computer connected to the private cloud[7]. The database MySQL is used to store the details of the learners, trainers and the contents used for E-learning system (Fig 1).

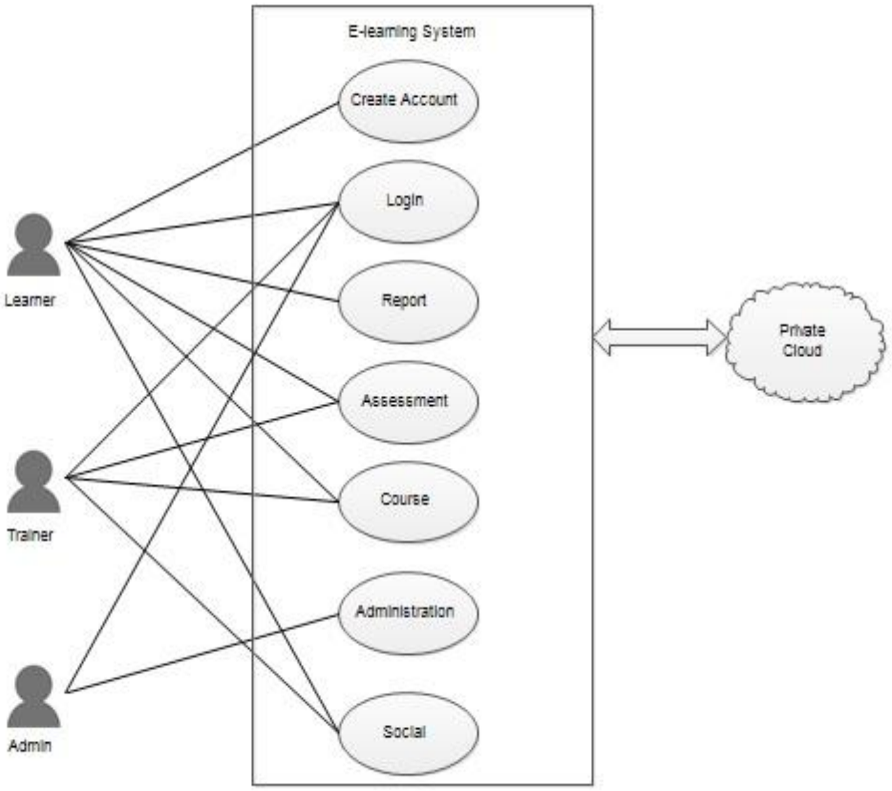

Fig 1 .E-learning system in private cloud.

The hierarchal attribute set based encryption access control technique is incorporated in E-learning system in order to restrict access over unauthorised users. The data are kept confidential for both students and trainers[8]. For securing the data, the proposed system has three keys that is private key, public key and master key. The encryption techniques uses public key, the decryption process takes both public and private key. For accessing the allowable data the master key is used. The scalability is achieved which manages the workload of trainers mapping with the students (fig 2).

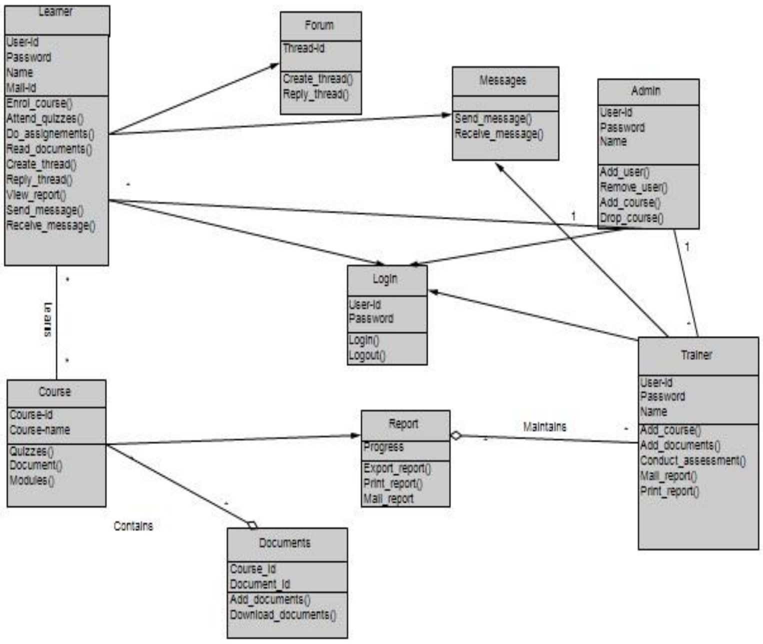

Fig 2 Class Diagram of E-learning System.

Key Gen(MKey, s, T): The user takes input as the master key (Mkey) which is the identity of user and attributes of key structure. It gives Privatekey PrKey for the user.

Encrypt (Pukey , M): The user takes public key (Pukey) and Message (M) as input and encrypts the messages for the resultant cipher text(CiText).

Decrypt(CiText, PrKey) : It takes Cipher text (CiText) and private key (PrKey) of user as a input and decrypts the message for original plain text.

Advantages of the Proposed System

- A flexible and Scalable tool for engaging trainers and learners.
- E-learning system in cloud ubiquitous environment.
- No need to store and backing up it from one device to the other.
- Allows learners to avail the E-learning resources from different places and can also access through different resources such as mobile, laptop and desktop computers provided that internet access is available.
- Restricted access control using three keys private, public and Master key.
- Learners can experience a secure, richer and diverse learning environment.
- It provides affordable and secure solutions to the academic institutions.
- Flexible, Secure and dynamically scalable infrastructure, which reduces the overall maintenance cost.

- This virtualized e-learning solution increases the performance and reduces overall cost and burden for the academic institution.

Building a Private Cloud

Eucalyptus is one of the most popular and leading open source private cloud platform which is used to create and manage a private cloud setup. It affords an Elastic Compute Cloud (EC2) Compatible platform as well as Simple Storage Service (S3) compatible storage platform.

Ubuntu Enterprise Cloud

The UEC (Ubuntu Enterprise Cloud), which is powered by Eucalyptus, is a very high Configurable and Customizable to a variety of environments. It is a private cloud set-up which is used to build up its own IT infrastructure. Using Ubuntu Enterprise Cloud, it is easy to bring the same self-service potential into the data center using the same APIs and tools used on Amazon Elastic Cloud.

Using UEC, you can easily deploy workloads and run immediately. The architecture of Ubuntu enterprise cloud consist of a frontend running with one or more Cloud Controller, Walrus, Cluster Controller, Storage Controllers with one or more nodes. The UEC cluster controller offers diverse virtual images (IaaS Services) in which the administrator want to create several OS images as a template. When a cloud user requests for a Virtual Machine.

The virtual machine (VM) is allocate into the suitable node Controllers with a configured VM image as an instance. Then the cloud user can execute necessary service onto the virtual machine.

Private Cloud Setup:

- **Server 1**: Install Ubuntu enterprise cloud. Installation mode: Cloud controller, Walrus storage service, Cluster controller and Storage controller.
- **Server 2**:

Install Ubuntu enterprise cloud Installation mode: Node controller

- **Exchange of Public SSH keys**:

On node controller setup a temporary password.

- **Get Credentials**:

On the Cloud controller, install credentials which consist of certificates and environment variables.

- Installation of images in Server1
- Finally Running Instances in cloud

Deployment of E-learning System in private cloud:

This paper focuses on all three deployment models such as platform as a service, software as a service and Infrastructure as a service using UEC. The E-learning application based on Hierarchical attribute set based encryption access control technique is developed using J2EE, a user can access E-learning application from any computer connected to the private cloud by using Apache web server. The database MySQL is used to store the details of the students, facilitators, and the content used for E-learning solutions.

Conclusion

Cloud computing is an IT centred emerging trend set for managing and affording resource as a services over the internet. The progress of cloud computing is rapidly shifting landscape of Information Technology to the long held pledge of utility computing into a reality .In this paper we developed an E-learning system with Hierarchical attribute set based encryption access control technique and deployed the application in private cloud using open source technologies like Eucalyptus and VMware.

The virtual machine images are available in the cloud, based on the user request and its instances are created. This proposed system achieves security, interoperability, scalability and quality of E-learning solutions.

References

1. Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012
2. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute based encryption," IEEE Symp. Security and Privacy, Oakland, CA, 2007.
3. V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data", ACM conference on Computer and Communications Security (ACM CCS), 2006.
4. M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure Atrribute-Based Systems", ACM conference on Computer and Communications Security (ACM CCS), 2006.
5. G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010
6. Lawanya Shri, M., Subha, S.," An implementation of E-learning system in private cloud",INTERNATIONAL JOURNAL OF ENGINEERING AND TECHNOLOGY,2013

7. Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, “Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption”, July 27, 2009

8. Dan Boneh, Xavier Boyen, Eu-Jin Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext”, Advances in Cryptology—EUROCRYPT 2005, volume 3493.

9. Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu, “Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts”, 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011.

10. Manoj Prabhakar, K.R., Lawanya Shri, M.," Implementation of an issue tracking system in private cloud", INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, 2014.

11. Tarun Kumar, K.S., Vignesh Kumar, P., Lawanya Shri, M.," An implementation of storage provisioning in private cloud",INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, 2014.

12. Deelman, rE., rSingh, G., Livny, M., et al. “Thercostrofrdoingrscience on the cloud: the montage example,” In: 2008 ACM/IEEE Conference on Supercomputing (SC 2008), Piscataway,NJ, USA, 2008, pp. 1–12. IEEE Press, New York (2008)

13. Neena Antony, A. Alfred Raja Melvin, “A Survey on Encryption Schemes in the Clouds for Access Control” International Journal of Computer Science and Management Research, 2012

14. Jang Hwang and Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu, “A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service”.

15. Jothipriya, G., Lawanya Shri, M.," Database synchronization of mobile-build by using synchronization framework",INTERNATIONAL JOURNAL OF ENGINEERING AND TECHNOLOGY , 2013

16. ZhangrGuoli, Liu Wanjun. “TherAppliedrResearchrof rCloud Computing Platform Architecture In the E-Learning Area,” Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on . Page(s): 356 – 359.

17. R. Buyya, C.S. Yeo, and S. Venugopal. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities, High Performance Computing and Communications, 2008,HPCC’08. 10th IEEE International Conference on, pages 5–13. IEEE, 2008 .

18. M. Armbrust, A. Fox, R. Griffith et al, Above the clouds: a berkeley view of cloud computing,Technical Report No. UCB/EECS{2009{28, University of California at Berkley, 2009, 1-23

19. I Foster, Y. Zhao, I. Raicu, S. Lu, Cloud computing and grid computing 360-degree compared, In Proc. of GCE'08, 2008 , 1-10
20. Deepa. M, Santhi. K, Malar,M.BB., Lawanya Shri. M “A character extraction technique based on character geometry using image processing”, INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, 2015.
21. Shiva Priya, K.P., Monisha, S.,Keerthiga, R., Lawanya Shri, M. , "A comparative analysis of classifier algorithm in defect prediction using cgbr framework", INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH , 2015.
22. M. B. BenjulaAnbu Malar[1], M. Lawanya Shri[2], *M. Deepa[3], K. Santhi[4] “Approach for Secure Authorized Deduplication using Hybrid Cloud “,INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, 2016.

Corresponding Author:

M. Lawanya Shri*,

Email: *kmlavanya@vit.ac.in*