International Conference on Recent Innovations in Science, Agriculture, Engineering and Management
University College of Computer Applications Guru Kashi University, Bathinda, Punjab (India)
20th November 2017, www.conferenceworld.in ISBN: 978-93-86171-80-1

Biometric Access of Cloud based E-Learning Content

Mir Saleem

[1]*Department of Computer Sciences, J&K Institute of Mathematical Sciences, Srinagar, J&K (India)*

ABSTRACT

With the help of networks/ internet, it is possible to adopt e-learning system at low cost. Problems related to the security issues render greater constraints for cloud vendors and users. Various combinations of signal transmission techniques, advanced web technologies and other hardware developments which establishes secure e-learning. Cloud computing, an application of computer networks, deserves a separate field for research due to its enormous applications like E-Learning. E-Learning methods are implemented with cloud computing technology to provide advantages to academic end users but can compromise in security. [1]

Proposed methodology ensures data availability and provides solution to secure data from attackers, by discovering security issues in cloud service delivery model with an aim to suggest a solution in the form of security measures related to the cloud based e-learning. Different types of attacks in service delivery models of e-learning proposed by different researchers are discussed. Threats, security requirements, and challenges involved are also taken into consideration. The basic intention is to develop this technology is to enhance the efficiency, utilization and performance of the computer resources but despite the enormous potential that is promised by this discipline is still to be fulfilled because of the various security issues.

In this paper we address the issue of access control to the E-Learning content on cloud by the use the biometric verification by using biometric iris verification for authentication of users.

Keywords: Cloud computing, access control, iris biometric, gray level co-occurrence matrix (GLCM).

I.INTRODUCTION

The concept of cloud computing has been evolving from many years. It is difficult to recall a topic that received so much hype as broadly and as quickly as big data. While barely known a few years ago, big data is one of the most discussed topics in business today across industry sectors. This work mainly focuses on the access of the e learning data that is retrieved by users of a certain organization. The access is obtained by customary login IDs and passwords by the organizations to their databases on a cloud. Since, passwords and IDs can be forgotten or misplaced and therefore misused to harm the e learning data. It, therefore, becomes very critical to control the access by some more reliable way and real possession by any person[2]. One solution of this kind is the use of human behavioral or physiological characteristics for getting an access to the critical data retrieved from a cloud. The biometric that we have proposed to be used and experimented in this work is the human iris. All humans have a unique iris pattern made up of furrows and ridges. It is this unique information about the person that can be used for access control. The algorithm for obtaining the useful information is discussed in the subsequent sections. With this method of providing access control and authenticating users protects the cloud

from various malicious attacks. Before going to the results and conclusion we define certain relevant terminology:

II. CLOUD SYSTEM

Cloud computing employs three service delivery models as listed below through which different types of services are delivered to the end user. Each service model has different levels of security requirement in the cloud environment. They are:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

These models provide Software, application platform and infrastructure resources as a service to the users. The Figure 2 shows the different types of attacks involved in these service delivery models.

The major security issues with cloud are:-

- Privacy and Confidentiality Once the clients outsource data to the cloud there must be some assurance that data is accessible to only authorized users. The cloud user should be assured that data stored on the cloud will be confidential.
- Security and Data integrity Data security can be provided using various encryption and decryption techniques. With providing the security of the data, cloud service provider should also implement mechanism to monitor integrity of the data at the cloud.[3]

III. DATA PROTECTION FOR THE CLOUD

Cloud and virtualization gives you agility and efficiency to instantly roll out new services and expand your infrastructure. But the lack of physical control, or defined entrance and egress points, bring a whole host of cloud data security issues – data co-mingling, privileged user abuse, snapshots and backups, data deletion, data leakage, geographic regulatory requirements, cloud super-admins, and many more.

IV. CLOUD DATA SECURITY CHALLENGES

4.1 Data Replication & Lack of Visibility

Snapshots and backups are taken daily, or even hourly, and automatically stored in the cloud. Do you know where they've been stored, or who can move and copy them? Can you trace unauthorized copying of data?

4.2 New Class of Privileged Users

Virtualization and cloud computing require cooperation between security, storage, server, application, and cloud security admins – all with access to your most sensitive data. With this number of people, the risks of failing an audit, or an admin going rogue, grow exponentially.

4.3 Data Loss from a Breach

In minutes, a disgruntled employee can load an entire virtual machine onto a thumb drive. Virtual data is easily lost or exposed as it moves between VMs or in the cloud. Can you prove that authorized users are accessing your data within their defined policies? Can you block access to compromised information?

4.4 Security in Public Cloud Environments

SafeNet identity and data protection solutions help organizations that want to utilize Amazon Web Services, Microsoft Azure, IBM Softlayer, and VMware public cloud environments as well as applications developed on the Cloud Foundry platform.

V.BIOMETRIC SYSTEMS FOR USER AUTHENTICATION

Authenticating the identity of users is a critical issue in information security. Biometrics is known for recognizing users based on their physiological or behavioral traits as identifiers and these cannot be easily stolen unlike passwords or ID cards. Biometrics could be employed as the primary means for authentication, called user identification, as well as a complementary (secondary) method for authentication, known as user verification. Biometric traits that cannot be easily forged and are supposedly unique for each user can form the basis of techniques for user identification. Biometric traits need not be unique for each user, but, can be used to validate whether a user is whom he/she claims to be form the basis for user verification techniques. The first half of the chapter describes several biometric techniques used for identification and verification and compares them with respect to different operating parameters. In addition, the different components (constituent blocks) of a biometric system and the performance metrics used to analyze the effectiveness of biometric systems are also discussed. The second half of the chapter focuses on the security aspects of biometric systems, especially spoofing attacks and a solution to enhance the security and effectiveness through multi-biometric systems.

VI. E-LEARNING

E-learning is electronic learning, and typically this means using a computer to deliver part, or all of a course whether it is in a school, part of your mandatory business training or a full distance learning course. E-Learning has developed, and now we embrace Smartphone's and tablets in the classroom and office, as well as using a wealth of interactive designs that makes distance learning not only engaging for the users, but valuable as a lesson delivery medium. E-Learning user can access the data in Cloud by using the Secured layer.

VII. PROBLEM FORMULATION

Users who put their large data files in the cloud storage servers can relieve the burden of storage and computation. At the same time, it is critically important for users to ensure that their data are being stored correctly and safely. So, users should be equipped with certain security means so that they can make sure that their data is safe. The major concern is the security of data at rest and while moving. So to handle this problem it is required that data at both user and server end

VIII. GLCM BASED FEATURE EXTRACTION

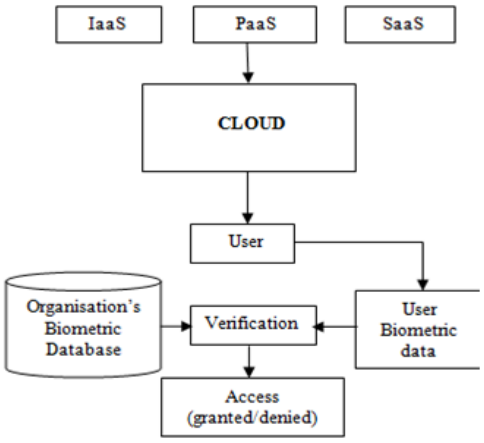

Figure 3: Proposed Access control model

The image feature extraction critical task in any machine learning applications in general and biometric verification in particular, based upon morphology/shape and texture features from an image by using appropriate extraction. I am proposing a method that uses iris for verifying the users on a cloud and considering that iris is very rich in the textural information, I chose to extract the textural features of the iris. The textural feature extraction methods are the oldest and the one of the most powerful statistical method. The different textural features that can be computed from an image are the co-occurrences matrices and run length analysis (long run emphasis, run length uniformity, run length non-uniformity, short run emphasis etc.). Here, however the textural features of iris for the purpose of verification of an authentic user are obtained by applying gray level co-occurrence matrix method. The Grey level co-occurrence matrix actually computes the number of occurrences of a particular gray level/intensity in an image. Other methods for computing the same gray level metrics include Gabor filters and wavelet analysis. These dependence metrics were first of all introduced by Julesz [8] for texture classification. Haralick [9] and Rosenfeld and Troy proposed two- dimensional spatial dependence of gray tones in a co- occurrence matrix.

Grey Level Co-Occurrence Matrix (GLCM) is one of the best known texture Analysis methods which takes advantage of the texture of an image. GLCM estimates image properties related to second order statistics. Each entry (i,j) in GLCM corresponds to the number of occurrences of the pair of grey levels i and j which are a distance d apart in the original image. The algorithm used for calculating gray level co-occurrence matrix is given below [11]. Typically, GLCM is calculated in a window

size that is small, which scans the whole image. The window is moved in along different angles and along the different inter-pixel distances "d". The number of features that can be calculated by applying GLCM is large but the features that we have calculate include entropy, correlation, variances, contrast, sum variances, Dissimilarity, Homogeneity, angular second moment. In the experiments that are carried during this work, a small value of "d" is used since iris has a soft texture: the gray level tone relationship between the pixels changes over small values of the inter pixel distance'd'.

 ISBN: 978-93-86171-80-1

IX. PROPOSED BIOMETRIC CLOUD ACCESS

By now, we have seen various aspects by which a cloud works i.e. deployment model used, delivery model used and the services provided. There are almost all the infrastructures in the world that use cloud services and all such critical infrastructures have security issues associated with them. Some of them are have been very abundantly discussed in the Literature and some are yet to be fully explored. Among all the issues, one that must be considered positively and seriously is the access control. Now whenever we talk about access control, we know humans distinct physiological and behavioral characteristics can be an apt choice for this purpose. As already said, ones physiological or behavioral feature can't be comprised that easily as compared to tokens, usernames, passwords etc. For this reason the access control that is proposed in this paper makes use of the human physiological characteristic for authentication purpose. As can be seen in the figure 3 below, the organization that makes use of the biometric authentication/verification maintains a biometric database of the employees along with other credentials. So now we have the true identities of the employees stored at the back end. Whenever the access to the data on cloud is needed, the person has to authenticate himself with the online iris biometric sensor. The iris sensor captures the iris image of the user and the image is preprocessed i.e., image is enhancement and noise in the image is reduced. The preprocessing of this collected information is done to enhance the image qualitatively. Once the image is preprocessed, the iris textural features are computed as given by the algorithm in the previous section. The features of each person are stored in the database as separate templates along with proper labels. Once a biometric database is made, we test the database using both genuine and imposter persons. A genuine person or user is one who is known to the system and an imposter is one who is not known to the system. We want to develop such a system which can properly authenticate all genuine users without falsely rejecting any of them. Similarly all non-genuine users should be rejected without giving any false access. During the testing phase the biometric iris image of the query is again captured and preprocessed. The feature template is computed and is matched with the database. The matching is done using Euclidean distance method. Based on the result of each Euclidean distance corresponding to each query, a decision is made whether access is to be granted or denied. Euclidean distance of zero would mean that the query is perfectly known to the system and he/she is a legitimate user. Similarly higher values of Euclidean distances would mean an imposter or an intruder is trying to get an unauthorized access.

X. RESULTS AND DISCUSSION

The iris biometric that is implemented in this paper uses textural features and the same have been computed for the standard iris database CAISA v1.0. The gray level co-occurrence matrix features are computed using MATLAB 7.9. The decision about the authenticity of any person is automated by developing a smart interfaced software system that links the incoming data from a cloud to the the user that has demanded for that access. Rather than using an old fashioned username ID and the password, the person's actual and inherent possession determines whether he or she is given to be an access. The inherent possession of a user here used is the iris. Since the iris of every human is unique, it really does eliminate the use of manmade username ID's and passwords determined by the Euclidean distance value computed at the matching level. The decision is made by

a predefined threshold value of the Euclidean distance. In this work, we have computed the correct verification rates at different thresholds as shown in the table 1.

The results are evaluated based on the minimum data access score obtained by the user. Whenever an access is needed by the user, the system automatically computes the access score that it obtains based on the captured iris image. If the Iris image gives a score in excess of the threshold, then the user is authenticated and if the score falls short of the threshold then the access to the data is denied. As shown in the table above, the best results are obtained when the threshold is selected as 30. Corresponding to this threshold the genuine access rate is 96.6 i.e., the percentage with which the biometric iris verification /authentication system can perform correctly is around 97 percent.

Table 1

Threshold and Recognition rate

Minimum Access Score (Threshold)	Genuine Access Rate (%)
60	77.2
55	77.6
50	79.3
45	84.5
40	87.7
45	91.2
40	93.3
35	94.1
30	96.6

XI. CONCLUSION

The proposed and implemented a novel method for the e-learning data access control on a cloud. The access of data is obtained by the online iris verification of the cloud service user. The features of iris have been computed using GLCM which is a technique based on texture and being known as one of the strongest and efficient second order statistical tool. There is plenty of work that has been carried on security aspects like data confidentiality on a cloud using some known encryption techniques and other security issues have also been dealt significantly but the access control of the data has not been given considerable attention. Our work focused on this area by using iris online biometric verification/ authentication of e learning data on the cloud. A standard database is used for testing the proposed algorithm. The results of the proposed scheme for authentication shows that it is a reliable method for access control, but there is still a room for improvement in terms of percentage of authentication rate.

REFERENCES

[1] M. Durairaj and A. Manimaran A Study on Security Issues in Cloud based E-Learning International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013

[2] Hamid Haqani ,Mir Saleem, Shoaib Amin Banday and Ab Rouf Khan - Biometric verified Access Control of Critical Data on a Cloud

[3] John Harauz. Lori M. Kaufman. Bruce Potter. "data Security in the World of Cloud Computing", IEEE Security and Privacy, v7, 2009,pp.61-64.

[4] ZHANG Hui.XING Peizhen. "Information Security Analysis in Cloud Computing Environment", Computer Technology and Development, v21(12),2011,pp.164-171.

[5] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing v14",Nat.Inst. Standards echnol.[Online].Available:http://csrc.nist.gov/groups/SNS/cloud-computing/index.html,2009.

[4] Iankoulova, I.; Daneva, M., "Cloud computing security requirements: A systematic review," *Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on* , vol., no., pp.1,7, 16-18 May 2012 doi: 10.1109/RCIS.2012.6240421.

[5] D. Firesmith, "Specifying reusable security requirements," J of Object Technology, 3(1), 2004, pp. 61–75.

[6] S.A. Almulla and C. Y. Yeun, "Cloud computing security management," ICESMA 2010, pp. 1-7.

[7] H. Sato, A. Kanai, and S. Tanimoto, "Building a security aware cloud by extending internal control to cloud," ISADS 2011, pp. 323–326.

[8] B. Julesz, "Visual pattern discrimination," IRE T M In~form, Theory, vol. 8, no. 2, pp. 84-92,Feb 1962.

[9] R. M. Haralick, "A texturecontext feature extraction algorithm 1241, Mar. 1973. for remotely sensed imagery,'' in Roc I971 IEEE Decisim and ConfrolConf. (Gainde, FL), pp. 650-657,Dec. 15- 17,1971.

[10] Banday, S.A; Mir, A.H; Khurshid, F., "Multi-Unit iris biometric fusion using grey level co-occurrence matrix features," Advanced Electronics systems (ICAES), 2013 International Conference

[11] on, Vol, no., pp.225,229, 21-23 sept,2013.