JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-4, Issue-04 E-ISSN: 2347-2693

Data Leakage Detection in Cloud Computing using Identity Services

K. Mythili[1*], S. Rajalakshmi[2] and D. Vidhya[3]

[1] Department of CSA, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University, India,
[2,3] Department of CSE , Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University, India

www.ijcseonline.org

Received: April/02/2016 Revised: Apr/10/2016 Accepted: Apr/22/2016 Published: Apr/30/ 2016

Abstract— The emergence of cloud computing paradigm offers attractive and innovative computing services through resource pooling and virtualization techniques. It shifts the delivery and maintenance of software, databases and storage to the internet, transforming them into Pay-As-You-Go (PAYG) services, which accessed through a small business user's web-browser. This technology introduces a new concern for enterprises and business organizations regarding their privacy and security. Security as a service in a cloud model integrates their security services into a corporate infrastructure. In corporate infrastructure it mainly concentrates on security systems developed to store and maintain documents over the cloud platform. The proposed work focused on the security platform to store and retrieve files on the cloud with onetime password protection. The main contribution of this research is to authenticate file while uploading and downloading from server with onetime password protection. The files are distributed to the employees of an organization by administrator and it can be downloaded by user with onetime password protection. This feature helps to secure the data before viewed by user or any unauthorized user who is act as a third party to that organization.

Keywords— ***Pay-As-You-Go, privacy and security, onetime password protection***

I. Introduction

The vast spread of Internet resources on the web and fast growth of service providers enabled cloud computing systems to become a large scaled IT service model for distributed network environments[2]. The main characteristics of a cloud environment are abstraction and virtualization which make the technology to be perceived and applied completely in a different manner compared with existing traditional distributed systems. In this cloud computing platform we face difficulties in the user identity and access control over files with limitations in a company or any organization. We should provide identity management and access control by using tokens to access cloud resources for registered entities. Such entities can be people, software processes or other systems. In order to give a proper level of access to source, the identity of an entity should be verified first, which is the authentication process that precedes the authorization process. Besides authentication and authorization processes, auto checking file logging mechanism should be used to keep track of all successful and failed operations and files sent and received through admin regarding authentication and access number of attempts not to exceed the limit of OTP entries by user in the application.

II. Existing System

For the development of security solutions vast challenges have been faced in the cloud computing environment. In particular, an organization faces challenges on files security and it tries maximum authentication over files while distributing to the user. Especially in software as a service the administrator has to distribute files to the employees to process the tasks and client process those request and resend to the admin when completed. When retrieving data user is not trust party and any third party can access data with that user id too. This may lead to data leakage and we cannot find out that exact user who communicates with third party that is through any guilt agent[1].

III. Proposed System

The proposed system provides security to overcome issues related to cloud environment which provides access to store and distribute data from cloud administrator to user or employees of a company[4]. It helps to protect the data from data leakage by tokenization of files before distributing and set the time bound for each and every file that particular user needs to download from the cloud storage. This formula protects the data leaked from guilt agent who act as a third party and security is provided using OTP (onetime password) generation which is an auto generated random unique number for every file when user or an employee make attempts to view the content of file. At the same time the OTP is generated for the count value of three for one particular file if attempts exceed more than three it automatically locks the file and it will send the duplicate file as like fake object to the user.

When these data is leaked out, then the companies are at serious risk. This system presents the data leakage detection from trusted third parties and provides an administrator to easily identify the third party by onetime password generation. This will help user to make better understanding of security issues in cloud computing environment.

IV. METHODOLOGY

This study is all about data leakage in cloud environment and we provide a security measures to overcome leakage problems. Data leakage can be detected using several methods and those methods provide security with the implementation of algorithms. We implement the concept based on security in data leakage over cloud environment with component model. This component is developed with the help of ASP.NET framework.

A. *Data Leakage Prevention with OTP:*

- This framework consists of tokenization of users and administrator distributes files to every user in the organization based on request.
- When the user is ready to view the file it is displayed by onetime password generation, if wrongly entered more than three times file will not displayed to the user.
- The files can be of type such as audio, videos, images, word, PowerPoint and etc., this method will improves the security by a valid registered user and any user from outside will not able to access the file.
- If any unregistered user make attempts to access the file it automatically locks the file and duplicate file only is sent to that user. This may lead to identify the third party easily through the guilt agent.
- The guilt agent is identified with this method efficiently and the algorithm plays a role on fake record which is duplicated by the file downloading model.

B. *Presumption Of Data Leakage Prevention With OTP:*

Through this application efficiency, authorization and authentication can be improved easily. The onetime password helps the number to be change over time to time and it cannot be incorporated with any other password. Then it leads to testing, each and every process can be tested with the valid inputs from the user. Thus the study provides a new methodology to improve the security over cloud environment. This methodology implementation is helpful in protecting data leakage from third party agent and provides security by adding fake object as duplicate file when a third party attempts to view the contents in a file which is the most crucial factor faced by an organizations over the years. It focuses on implementation of a project to be associated in a form of applications which is already available and provides the unique model to improve security.

V. IMPLEMENTATION

In this study we tested in all phases such as, the login can be done based on the role of user selections, the user may be an administrator or a user who is registered with the organization. If the role selection is completed then it moves to next level. Then the fields are validated in the registration form, the mandatory fields have to be filled by the user who is new to the process. Then in another phase the unit testing is done with key values of uploading a files i.e., admin make an attempt to distribute the files to the user.

Then a random number is generated when a user has a necessity to view the file content, and in the mean time this auto generated random password is displayed in the message box. Then user should enter the password and not exceed more than three attempts. When the attempts exceed more than three, the file will be locked automatically from a user and it is removed from a user area. Table – 1 shows Test cases for unit testing.

Test No.	Test	Expected Result
1	If user gives invalid password	Error: Invalid password
2	If user gives valid password	Login is successful
3	If random password exceed three attempts	File will be locked and removed from a user area.
4	If password is correct before three attempts	User can able to view the content of a file.

Table - 1

A. *Validation Testing*

Validation is done for all forms where the process is gone through, in a first step when a user, who makes attempts to login without selecting a role, then a message shows to select a role. Then it continues the process. The distribution of file can be done when the role selection is an admin, then only files are distributed to the users who are registered.

By the next step validation is to be done for the tokenization of user identity when a user logs in, it will display the files which are distributed from the admin. The most important of validation is about the onetime password generation, when a user makes attempt to view the file without entering a valid number in the field allocated for that. Table – 2 shows test case of upload files for validation testing.

Test No.	Test	Expected Result
1	Attach File is Mandatory	Error: Choose file to upload
2	Wrong File Format is Chosen	Error: Choose Correct File Format
3	Valid File No	Displays: File No Already Exists

4	Attempt to view file without OTP	Error: first enter the valid OTP number
5	If count more than three times	Displays: attempts exceeded

Table – 2

VI. RESULTS

The goal of the experiment was to see whether fake objects are accesses from the distributed data sets yields significant improvement in our chances of detecting a guilt agent. After that we evaluate onetime password technique to detect the data leakage and it helps to prevent the data to be leaked.

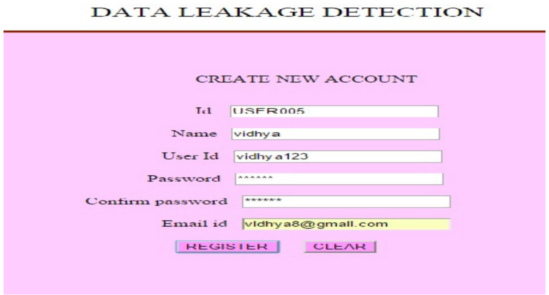
The overall evaluation of the proposed detection system is done from two perspectives:

- Integration - Integration demonstrates how the proposed security services can be integrated within a cloud environment.
- Security - Security demonstrates how securely the services are delivered to service requesters.

A. Advantages Of Data Integrity In Cloud Environment

1) Identity Management

Every enterprise will have its own identity management system to have access control of its information and computing resources. Cloud providers either integrate the customer’s identity management system into their own infrastructure, using federation, or a biometric - based identification system, or provide an identity management solution of their own.

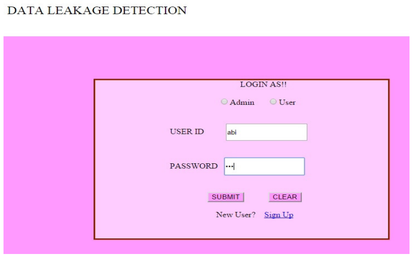

DATA LEAKAGE DETECTION

CREATE NEW ACCOUNT

Id: USER005
Name: vidhya
User Id: vidhya123
Password: ******
Confirm password: ******
Email id: vidhya8@gmail.com

Figure – 1

The above figure – 1 demonstrates the registration of a new user for an organization with the required details. Once the registration is completed the user details are stored in database. In case the user needs to update the details by logging in with the user id and password and can change or modify the entered details. In registration all the fields entered are mandatory. For the registered users only files are distributed from an admin.


DATA LEAKAGE DETECTION

LOGIN AS!!

○ Admin ○ User

USER ID: abi
PASSWORD: •••

Figure – 2

The above figure – 2 explains about the login for the user, the user must login to access the application. Before logging in the user must select a role either admin or user. This is done for the security purpose, because an admin and user access the application. Both the login roles have separate login forms and take to different pages so they must select a role to access. It links the confidential information of the users to their enrollment process and stores it in a cloud database of an organization. Making use of this technique, identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.

2) Physical Security

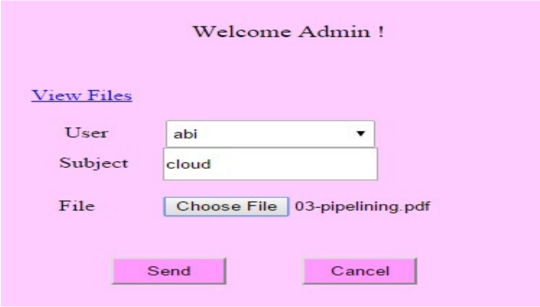
Cloud service providers physically secure the IT hardware such as servers, routers, cables etc., against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' i.e., professionally specified, designed, constructed, managed, monitored and maintained data centers.

3) Personnel Security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.,

4) Availability

Cloud providers help to ensure that customers can rely on access to their data and applications; at least in part failures at any point - not just within the cloud service providers' domains - may disrupt the communications chains between users and applications.



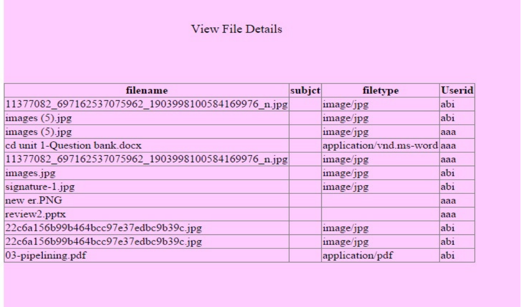
User: abi ▾

Subject: cloud

File: Choose File 03-pipelining.pdf

Figure – 3

The above figure – 3 states that the admin views of application, after login by admin this from will be shown. Admin need to distribute the files to user, all the user names who have registered will be displayed in user list. Then subject for the reference of a file should be mentioned, then admin upload a file by clicking on the upload button and send to the particular user.



filename	subjct	filetype	Userid
11377082_697162537075962_1903998100584169976_n.jpg		image/jpg	abi
images (5).jpg		image/jpg	abi
images (5).jpg		image/jpg	aaa
cd unit 1-Question bank.docx		application/vnd.ms-word	aaa
11377082_697162537075962_1903998100584169976_n.jpg		image/jpg	aaa
images.jpg		image/jpg	abi
signature-1.jpg		image/jpg	abi
new er.PNG			aaa
review2.pptx			aaa
22c6a156b99b464bcc97e37edbc9b39c.jpg		image/jpg	abi
22c6a156b99b464bcc97e37edbc9b39c.jpg		image/jpg	abi
03-pipelining.pdf		application/pdf	abi

Figure – 4

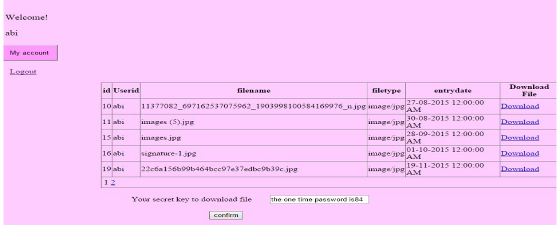
The above figure – 4 shows that the files distributed by the administrator to users, the filename tells the name of a file or a document and the subject displays that while sending file to user admin mentioned some text about the files. Then file type tells about type of file which is send to user and at last the user id is the name of the user who receives the file from admin.

5) Application security

Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.

6) Privacy

Providers ensure that all critical data such as email id and account number are masked or secured and that only authorized users have access to data in its entirety[5]. Moreover, digital identities and credentials must be protected as should any data in the cloud.

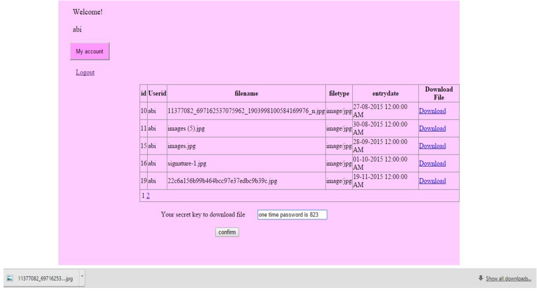


id	Userid	filename	filetype	entrydate	Download File
10	abi	11377082_697162537075962_1903998100584169976_n.jpg	image/jpg	27-08-2015 12:00:00 AM	Download
11	abi	images (5).jpg	image/jpg	30-08-2015 12:00:00 AM	Download
15	abi	images.jpg	image/jpg	28-09-2015 12:00:00 AM	Download
16	abi	signature-1.jpg	image/jpg	01-10-2015 12:00:00 AM	Download
19	abi	22c6a156b99b464bcc97e37edbc9b39c.jpg	image/jpg	19-11-2015 12:00:00 AM	Download
1 2					

Your secret key to download file: the one time password is84

Figure – 5

The above figure - 5 displays the screen after login by the user. It shows only the particular user list for security issues. The files received will be displayed in a grid view and shown the time of sending from admin. The download option is provided for every document to view the content of a file. But when an attempt to download a file the onetime password will be displayed and user should enter the correct password to download the file.



id	Userid	filename	filetype	entrydate	Download File
10	abi	11377082_697162537075962_1903998100584169976_n.jpg	image/jpg	27-08-2015 12:00:00 AM	Download
11	abi	images (5).jpg	image/jpg	30-08-2015 12:00:00 AM	Download
15	abi	images.jpg	image/jpg	28-09-2015 12:00:00 AM	Download
16	abi	signature-1.jpg	image/jpg	01-10-2015 12:00:00 AM	Download
19	abi	22c6a156b99b464bcc97e37edbc9b39c.jpg	image/jpg	19-11-2015 12:00:00 AM	Download
1 2					

Your secret key to download file: one time password is 823

Figure - 6

The above figure – 6 shows that the onetime password is generated and the user entered the password within three attempts. The file is download from the database then, the content of a file can be displayed to the user. This ensures the security of a file from the third party and hence the file is prevented from a data leakage in an organization. This leads to the security and the method implementation through the component developed to prevent the issues over the data leakage.

7) Cloud Security Controls

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories

a) Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

b) Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure[3].

VII. CONCLUSION

This research has proposed a cloud security system and based on this concept, contributions are made in the area of authentication and authorization services for a cloud environment. Our proposed model helps to various users and provides secured connection between the environments. Onetime password is provided with the time bound for viewing the files contents, the guilt agent model process with authorization and authentication. The problem has been solved and the goals have been achieved to prevent data loss with the onetime password generation and efficiency of data access has been improved with above mentioned methodologies.

VIII. FUTURE WORK

In this research a cloud security system has been designed for managing authentication and authorization services applying quite new cloud service paradigm, such as Security as a Service. The proposed system supports delivery of data based on two identity services. Therefore, more identity service features can be added, such as single log out, session Refreshment, etc. The prototype implementation has some limitations: user can be signed by selecting role at a time, there is a policy set concept applied for this system, and there is no separately implemented profiles for a registered user. Therefore, more features can be added to the prototype authorization system. Besides, a prototype of authentication system can be implemented according to the designed system.

REFERENCE

[1] Papadimitriou P and Garcia-Molina, “Data Leakage Detection” Knowledge and Data Engineering, IEEE Transactions on Volume: 23, Issue: 1, Page No (51-63), Jan 2011.

[2] Michael Miller, “Cloud Computing - Web-Based Applications that change the way you work and Collaborate Online” , Pearson Education, 2012 .

[3] Kumar Ajay, Goyal Ankit, Kumar Ashwani, Chaudhary Navneet Kumar and Sowmya Kamath, “Comparative evaluation of algorithms for effective data leakage detection”, Information & Communication Technologies (ICT), 2013 IEEE Conference, ISBN 978-1-4673-5759- 3, Page No(177-182), April 11-12, 2013.

[4] Chandni Bhatt et al, “Data Leakage Detection”, International Journal of Computer Science and Information Technologies, 2014

[5] Ankit Tale, Mayuresh Gunjal and B.A. Ahire, “Data Leakage Detection Using Information Hiding Techniques”, International Journal of Computer Sciences and Engineering, E-ISSN : 2347 - 2693, Volume-2, Issue-3 Page No (155-158), March - 2014.