RESEARCHERID
THOMSON REUTERS

[ICRTCET-2018]

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ACCESSING DATA IN CLOUD PLATFORM USING IDENTITY AND PROVIDING STRONG SECURITY, AUDITING BASED ON IBDO SCHEME

Bhavya Shree M N[*1], K S Ananda Kumar[2], Kavyashree S[3], Gagana H[4] & S Geetha[5]

[*1,3,4&5]Information Science and Engineering, Rajarajeswari College of Engineering, Bengaluru, India

[2]Asst. Prof, Information Science and Engineering, Rajarajeswari College of Engineering, Bengaluru, India

ABSTRACT

— The main aim of using cloud platform to store information is that, it provides large space for storing files and facilitates all types of services to individuals and organization. To achieve high security, distributed sharing services and auditing concerns on storage files, we develop an identity-based data outsourcing (IBDO) scheme which provides most important and beneficial features. The advantage of using IBDO scheme: First, IBDO scheme permits a file owner to give permission only to the dedicated user to transfer a data to a cloud storage server on their behalf, so that the dedicated proxies are identified and given permission to upload files to a cloud based on identity. Second, IBDO scheme provides strong security by using efficient algorithms. It quickly finds out unauthorized person who tries to make modification on storage files. It also finds misuse of authorization. Third, IBDO scheme provides strong auditing mechanism in which auditor can run the auditing protocol to detect file origin and type.

Keywords: *auditing protocol, cloud storage, distributed clients, IBDO scheme, security.*

I. INTRODUCTION

Cloud platform host different remote servers to store, manage, and process data on the internet, unlike the local server or a computer. A person located in any part of the world can get in contact with different resources in the cloud and will be able to access it. Cloud computing is a mass storage area where many files can be stored in, and also files can be accessed by the end-user. For performing any action on the files, internet is the main source required. Hence, this can be called as the Internet-based computing. Also, cloud platform provides strong security on the files that are stored in the cloud therefore; it is a powerful storage area. So, the individuals and organizations rely on such storage services. An example of a Cloud Computing is Amazon Web Services (AWS). Amazon owns a cloud and provides the customers with storage, computations, and applications.

Identity-Based Data Outsourcing is one such scheme where it provides strong security to the files present in the cloud platform. Let us relate IBDO scheme to the real scenario of a college where, Identity Based refers to recognition of a student through College ID, Data is the information of a student maintained by the college and Outsourcing connects student's details from college to the respective university. In this scheme, certain operations (storing, accessing, updating) are performed on the files by the end-user using the authentication provided by the data owner. Identity refers to recognizing dedicated proxies based on their authorization by login ID.

ISSN 2348 – 8034
Impact Factor- 5.070

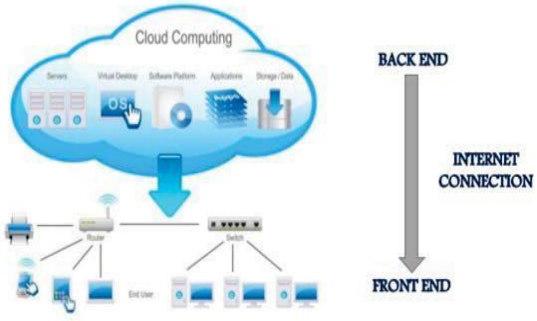

Figure 1: Architecture representing the working of cloud platform

Cloud architecture represents the operation of the cloud as in Figure 1. Cloud provides a back end computing where services like storage, Virtual desktop environment, multiple applications, and different types of operating systems are provided. In the front end, it is possible to obtain the services of the back end on different applications such as laptop, personal computer, and also on mobile phones. But this can be possible in the presence of the internet connection. So, the routers and switches are used to connect the front end with the back end.

II. RELATED WORKS

Wang discusses about the cloud computing as to prove the server as an auditor of integrity for a data in a file of storage. Auditor is the third party of this system, except the data owner. Therefore the integrity is proved on the information which is available on the open source. This implements the data to be verified without downloading the data of whole document for the clients. Data stored in multi-cloud servers in the previous discussions or applications and the efficiency of the integrity protocol must be proved to gather or store the cost of the verifiers. This protocol is much secured in many problems that are in standard such as computational Diffie-Hellman problem. A major advantage is flexible and efficient. It proposes to realize a verification done for public, private and delegated clients [1].

Cloud platform is a mass storage where we store and process large amount of information. Social Medias like Face book, Whatsapp, Gmail where large amount of information will be processed and updated per hour throughout the world in an unimagined way. So the challenging task is providing security to the data stored in cloud platform. In this paper we mainly focus on systematic security analysis while sharing data. This paper illustrates that data owner uploads file to cloud and he can give permission to his employees, so that the employee will have access to the cloud by making use of different sharing methods.

Public sharing: In this type of sharing, URL designated to access the particular folder is available. So, anyone can use this URL to access the data.

Secret sharing: In this type of sharing, cloud service provider will generate URL. If data owner has to share data with end user, then this URL is shared to particular end user, only then end user can access those data. After getting URL there is no further authentication asked.

Private sharing: In this type of sharing, data owner has to tell who can access the data which is been shared. Then, the end user will be validated by cloud service provider by allowing the end user to sign in through the account. End user who wants to access the data has to maintain account with cloud service provider [2].

Normally storage services like compact disk, floppy disk, hard drives, and USB flash drives are used to store large amount of information. But these storage devices has limitations like storage capacity, cannot access the information from anywhere and anytime, less security and cannot provide fast access. So, the solution is to explore a new platform called cloud platform where bulk of information , different types of files ,images can be stored. Accessing

the data in cloud platform has many advantages like fast access, data can be accessed from anywhere and anytime. In this paper, we introduce data protection as a service which mainly focuses on providing security or protection for entire applications and data stored in cloud platform. So that this reduces the cost and risk of developing and implementing security schemes for individual applications [3].

III. IMPLEMENTATION

The modules co -ordinate themselves to help out the Identity-Based Data Outsourcing (IBDO) scheme perform certain actions on the file. Hence, the modules are listed below,

- Data Owner
- Proxy Server
- End User
- Cloud Server
- Third-Party Auditor
- Attacker

Data Owner, Proxy Server, Third-Party Auditor are the ones' who rely on the cloud storage so, they are addressed to be the cloud-clients. End User is the one who is gaining benefit of the cloud by cutting down the cost on PC and it's peripherals; he/she will be able to access the files that requires from the cloud storage itself. Cloud Server is the home for all files storage. Third-Party Auditor is the trusted person who works for the file owner. Attacker is an external or an internal person who comes in contact with the files present in the cloud server; he/she can make changes to the file. Through these modules IBDO scheme is able to provide the following distinguishable features:

- Identity-Based File Outsourcing
- Third-Party Auditing
- Strong Security Provisioning

Identity-Based File Outsourcing: The cloud-clients which include file owner, proxy server, and third-party auditor are recognized by registering themselves in the particular cloud service provider such as Amazon Web Services (AWS) so they can find their identities by the ID. This ID means the identification of the cloud-clients in the particular cloud service provider. This helps our scheme to delegate the multi-user community efficiently.

Third-Party Auditing: This turns out to be the most unique part of IBDO scheme where the third-party auditor gets hold on the files when it is attacked. Then he/she audits the hacked file and sets the file back in track. Also, when the end user by chance attempts to enter a wrong user name or password he/she is not permitted to login further. Auditor has to then validate the user so that he/she can smoothly function over the login.

Strong Security Provisioning: Outsourced file can be detected with the unauthorized modifications using the security provided. Misusing/abusing of files is also eliminated using this security provisioning. Both this properties are taken care against the malicious agent who refers to be the attacker.

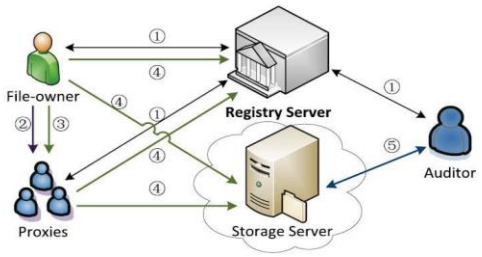

Figure 2: The Architecture of IBDO System

A. Data Owner

The corporate world beholds many files that have to be stored in its own company database. But, the data can be easily hacked by the hackers as it is having poor security norms. Also, it requires the computer system and the related peripherals for computing and maintaining the database which is costlier. So the trending solution to all such problems is the cloud computing. Hereby the IT world has shifted their files storage to the cloud platform.

Data Owner creates his profile through the Sign Up page to register to the cloud. Data Owner being the owner of the file has to register to the cloud to upload and manipulate the files. Once the registration is done in the cloud he/she can Sign In to the account, using the username and password. Data owner has a registration page where he/she has to provide details in brief. As Data Owner plays a vital role in uploading, editing and deleting of files. Once clicked on the submit button there is registration successful message that can be seen on the registration page for data owner to prove his identity. On successful registration data owner enters the login page and there he/she can provide their choice of login name and password. Then press on the submit button to enter the page. If the data owner has already registered then he/she can directly login to the page. As Data Owner enters the further pages there will be certain operations that can be performed such as, choose files for Upload, View files, Logout. When clicked on the choose files for upload option, there he/she is able to find a text box so they can enter the file name that can be uploaded. Data owner plays a unique part by providing extended authority to the proxy. So, the data owner has to select the particular proxy to whom he/she can provide the further authority on the files that they want to upload. By clicking submit it provides the authority to the particular proxy. Also data owner can view files that have been uploaded and on clicking on go back button they can switch to the previous screen and then finally logout.

B. Proxy Server

There will be a multiple authorized proxies who have registered in the cloud and are controlled by the data owner. Each proxy will have its own registration and login through which they can register into the cloud. The data owner will select authorized proxy and instruct proxy to upload a particular file. The main task of proxy is to upload a file which is indicated by data owner to the cloud. The auditor keeps track of proxy activity. If any dispute is made by proxy auditor will validate file. Proxy is the trusted person whom the data owner beholds. This bonds the positive relationship between them so that the data owner can share files with the proxy. On behalf of the data owner proxy uploads the file to the cloud. So, this masks the details of the data owner. There can be several proxies who can register themselves and they must be trusted proxies to the data owner. Once the proxy clicks the submit button it is successfully registered and the same message pops on the screen. Like data owner even the proxy has the login page. So, there he/she has to set their choice of login name and password and use it every time as they log in to this particular page. If Proxy already owns a login name and password then it can be used for further actions. As proxy enters the account then the following actions can be performed, Upload files, View files, Logout. For uploading of files to the cloud the proxy has to click on the link that is, upload files. From the choose file he/she selects the file that has to be uploaded and clicks on submit button. Then in the status window it will print a file uploaded successful message. So, this is an acknowledgement to the proxy for successful upload of file. If the file is not uploaded completely then in the status window it prints as unsuccessful file upload. Then they have to retry the process of uploading. In the view file link, the proxy can find the list of files that has been uploaded to the cloud by the proxy. Then they can click on go back button to see if any other file has to be uploaded else they can click on logout and return from the account.

C. End User

Operations of End User is shown in Figure 3. Each end user will have its own registration and login through which they can register in the cloud. When the data owner upload files to the cloud, based on the user requirement the files can be downloaded by various users at the same time. If the end user wants to download and access the file which is uploaded by the data owner, they request for a secret key. By using this secret key they can download the file. The file will be in encrypted form before downloading. After downloading, the file will be decrypted automatically by using AES algorithm. The end user will not have rights to make modifications to the content of the file. End user activity is tracked by auditor, if they make any disputes the auditor validates the file until which end user can not view and download that file. End user is the beneficiary person because they can obtain the benefits of downloading the files of their requirements from the cloud directly. So, from this he/she is also able to cut off the expenses

required to store the files on their own computer system. End user can first see the home page with link for user login and several other login pages link. To access the cloud services end user firstly has to register themselves in the cloud to obtain their identity. Once end user is registered there is a registered successfully message that pops up to ensure authentication. Then end user enters the login page, through this page he/she is able to obtain the further control on future pages.

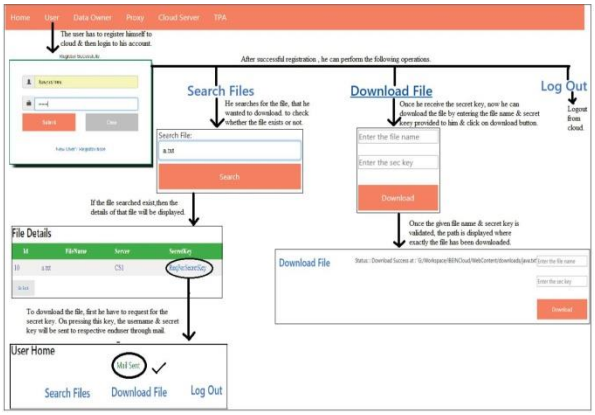

Figure 3: Downloading Process

In the login page end user has to enter login name and password of their choice. If end user already holds an account which means he/she has already registered, then they can login directly with login name and password. As the end user provides login name and password, they enter to the page of control which is the user home page. In the login page they can perform certain operations such as, Search file, Download file, Logout.

User can enter the filename that is required in the text box given in the below link, search file and press the button search. If the requested file is present in the cloud, then that particular file details is displayed on the end user screen. He/she can then click on go back button and download that particular file and finally logout. Once the proxy uploads the encrypted file to the cloud, the encrypted file gets stored in AWS cloud and this file can be accessed by end user. Before downloading the file, end user searches a file to check whether file exists or not. If exist, the end users request a secret key in order to download the uploaded file. When they click on download file, there they have to enter the filename which wants to be downloaded along with the secret key provided through mail and clicks on submit. If the entered key is valid, then the selected file will be downloaded and also the path where the file is downloaded will be displayed. By using this secret key the file will be decrypted and the end user can download the file. The end user does not have permission to make changes to the original file instead; he/she can make changes to the copy of that file.

D. Cloud Server

Cloud server is the one who provide the services to data owner, proxies, end user. Additional capacity can be temporarily used whenever the user needs. The cloud server will have user name, user id as identity through which they can login to the cloud. The cloud server will keep track of data owner, proxies, end user, auditor activities to provide a security. Cloud server will have the authority to view stored files, secret key, and attacker.

E. Third-Party Auditor

Third Party Auditor (TPA) is the one who monitors the files present in the cloud. So, he/she is the trusted person under the cloud server. TPA also keeps track of the end user and data owner account because if an invalidated malicious agent gets a chance to use the account of end user or data owner and manipulate the data. In such case the data becomes totally insecure and hence require the TPA. TPA does not have a registration page because as they work for the cloud server to prevent the data from malicious attacks. They do the work assigned by the cloud server. TPA has a direct login to the account and provide the login name and password. On submitting that page, the control goes to the personal page where they can perform the following actions, Validate files, Validate users,

Logout. TPA can choose validate files option in order to check the file for providing security. If the file is uploaded by an authorized data owner then such files are validated and the safe status is issued. If TPA finds an unsafe file then that particular file gets blocked and also there is no further access over that file to the end user. TPA then looks through the database where the registration of each and every end user is stored. If TPA finds the end user details in the database then, validates the end user and provides another chance or else the end user is blocked forever. After completing the task assigned to TPA, he/she can finally logout from the account.

F. Attacker

Attacker is an unauthorized person who tries to damage the original data or add some malicious information to files. The attacker will have only login page through which he/she can login to the cloud. When the Attacker Log in to the page he/she gets in touch with many files which is in encrypted form, so he/she adds some unwanted data to the encrypted form. Then the file status will be changed from safe to attacked. All these activities will be tracked by auditor and attacked file will be blocked, so that it is not visible to attacker. Once the auditor validates the file, the file will be safe and available to use.

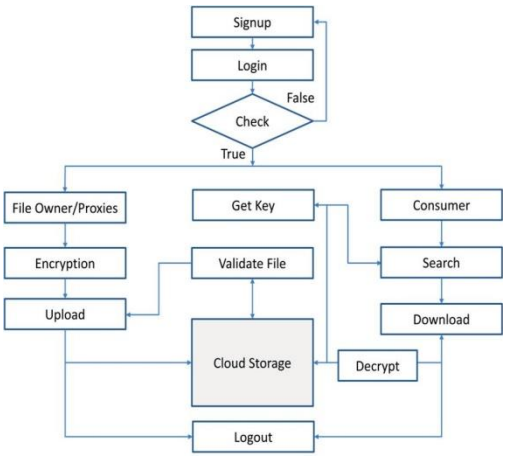

Figure 4: Flow Chart for IBDO Scheme

The cloud platform consists of five entities, such as data owner, proxy, end user, cloud server, and third party auditor as shown in Figure 4. Each entity plays an important role and each entity will have their own characteristics and responsibilities. Each of these entities will have separate sign up and login page through which they can login to their account. If an entity enters valid username then it results in successful login and can proceed to perform further activities, otherwise it results in unsuccessful login and the entity cannot perform further activities. If the data owner login is successful, he can choose proxy to upload the file, and select which file to upload. Before uploading the file will be encrypted. After uploading, the files will be validated by auditor. If the end user login is successful, he request for secret key. After getting secret key, the file will be decrypted ,then he search the particular file and download that file. After performing all the entities each of them will have logout operation through which he can exit.

IV. RESULTS & DISCUSSION

The IBDO scheme provides identity to data owner, proxy, end user, cloud server, auditor through which they register and login to the cloud. Making use of proxies will hide the details of data owner. So that attacker does not get to know it, which leads to high security. IBDO scheme involves generation of file key and content key which is used to provide a authority/permission to end users in order to access file. Multiple end users can search and download the files in the cloud platform in a more secured manner. This scheme involves auditing mechanism, auditor keep track of proxies, end users, attackers and determine file origin and file type.

ISSN 2348 – 8034
Impact Factor- 5.070

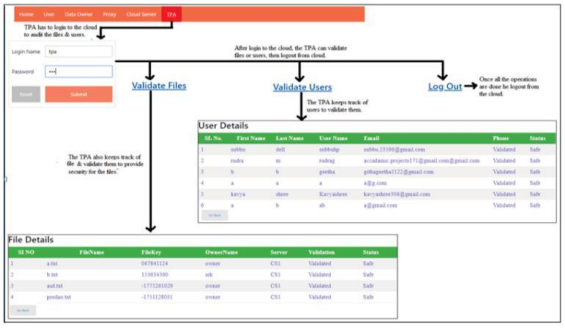

Figure 5: Work Flow for TPA

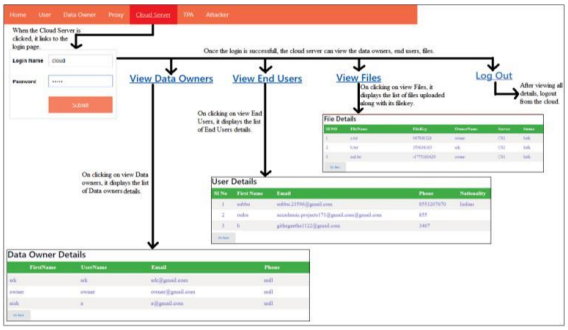

Figure 6: Work Flow for Cloud Server

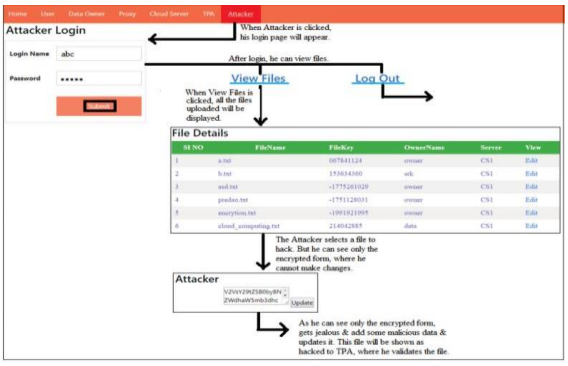

Figure 7: Work Flow for Attacker

V. CONCLUSION

In this paper, the data owner stores the files into the cloud where multiple end-users can access those file. Here we use Identity-Based Data Outsourcing (IBDO) scheme which provides high security, auditing for storage of files. The data owner selects a suitable proxy from the multiple proxies. The selected proxy can view the files and upload it to the cloud on owner's behalf. The uploaded file will be encrypted automatically using AES algorithm and stored into the cloud. The user can search and download the files by first making registration to the cloud and then can login to the cloud. The user requests for a secret key or file key to download the file. The secret key is sent to the user email id through which he/she gets permission to download that file. The third party auditor keeps track of the users and also validates the files. For each and every request of a secret key, new and different keys are generated only to secure the files from misusing.

Whenever an attacker tries to hack the file, only the encrypted form is visible, if they make any changes to encrypted code, the auditor will keep track of it, block the file that means it won't be visible to end user until that file is validated by the auditor using the content key or hash key generated based on the content of the file. At last by making use of IBDO scheme, AES algorithm and by auditing the files data will be more secured in the cloud.

VI. ACKNOWLEDGEMENT

The authors would like to express sincere thanks for encouragement and constant support provided by the Management RRGI, Dr. R Balakrishna Principal, Dr. J Amutharaj HOD ISE, RajaRajeswari College of Engineering, Bangalore-74, India during this research work.

REFERENCES

1. *Wang, Huaqun. "Identity-based distributed provable data possession in multicloud storage." IEEE Transactions on Services Computing 8, no. 2 (2015): 328-340.*
2. *Chu, Cheng-Kang, Wen-Tao Zhu, Jin Han, Joseph K. Liu, Jia Xu, and Jianying Zhou. "Security concerns in popular cloud storage services." IEEE Pervasive Computing 12, no. 4 (2013): 50-57.*
3. *Song, Dawn, Elaine Shi, Ian Fischer, and Umesh Shankar. "Cloud data protection for the masses." Computer 45, no. 1 (2012): 39-45.*
4. *Yang, Kan, and Xiaohua Jia. "Data storage auditing service in cloud computing: challenges, methods and opportunities." World Wide Web 15, no. 4 (2012): 409-428.*
5. *Wang, Huaqun, Qianhong Wu, Bo Qin, and Josep Domingo-Ferrer. "Identity-based remote data possession checking in public clouds." IET Information Security 8, no. 2 (2013): 114-121.*
6. *Yu, Yong, Man Ho Au, Yi Mu, Shaohua Tang, Jian Ren, Willy Susilo, and Liju Dong. "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage." International Journal of Information Security 14, no. 4 (2015): 307-318.*
7. *Zhang, Jianhong, and Qiaocui Dong. "Efficient ID-based public auditing for the outsourced data in cloud storage." Information Sciences 343 (2016): 1-14.*
8. *, Giuseppe, Roberto Di Pietro, Luigi V. Mancini, and Gene*
9. *Tsudik. "Scalable and efficient provable data possession." In Proceedings of the 4th international conference on Security and privacy in communication netowrks, p. 9. ACM, 2008.*