ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Protected Data Reserve over Cloud

R.S.Thakur[1], Ashwini Palghamol[2], Devashri Gaikwad[3], Gunjan Rakhunde[4].

Professor, Dept. of CSE, Dr. Babasaheb Ambedkar College of Engineering and Research, Maharashtra, India[1]

Researcher, Dept. of CSE, Dr. Babasaheb Ambedkar College of Engineering and Research, Maharashtra, India [234]

ABSTRACT: Cloud-based outsourced storage relieves the client's burden for storage management and maintenance by providing a comparably low-cost, scalable, location-independent platform. However, the fact that clients no longer have physical possession of data indicates that they are facing a potentially formidable risk for missing or corrupted data. To avoid the security risks, audit services are critical to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an un-trusted server, can be used to realize audit services.

Cloud computing has been emerged solution to the rising storage costs of IT industry With the high costs of data storage devices as well as the rapid rate at which the data begins generated it proves costly for enterprises or individual users to frequently update their hardware Apart from reduction in storage cost the user’s data to large data centres, which are remotely located, on which user does not have any control.

KEYWORDS: Cloud, cryptographic technique

I.INTRODUCTION

In order to avoid client burden cloud based outsource is used .Which help in storage management and maintenance by providing low cost, scalability, independent platform base location comparatively. The main fact client does not have control of data because facing dangerous risk of outsourced data. To avoid this risk, critical to protect integrity and availability of outsourced data. The encryption technique that data owner use over network makes secure data transmission. Outsourced data in cloud and computation results are not always trustworthy because data owners lack physical possession and control over the data as a result of virtualization, replication, and migration techniques. Protecting outsourced data from security threats has become a challenging and potentially formidable task in cloud computing; hence, many schemes have focused on ameliorating this problem and on enabling public audit ability for cloud data storage security. These schemes drop into two categories: total computation cost and burden on client side. Researchers have used bilinear map technology with public key cryptography. Although this technology is highly efficient, computation time is long and overhead cost is high. The client needs to perform numerous computations to ensure the integrity of data storage. To reduce auditing cost, we propose an efficient and robust scheme to maintain data integrity in cases that involve public auditing. Our scheme adopts modern cipher cryptography with a cryptographic hash function.

II. RELATED WORK

The notion of public auditability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. In, a public auditability model called Provable Data Possession (PDP) is presented for ensuring possession of files on untrusted storages. The PDP model employees the RSA-based homomorphism authenticators for data auditing. By using the PDP model, public auditing is achieved, but that model only supports static data. In subsequent work, the authors in present partially dynamic version of the PDP model.

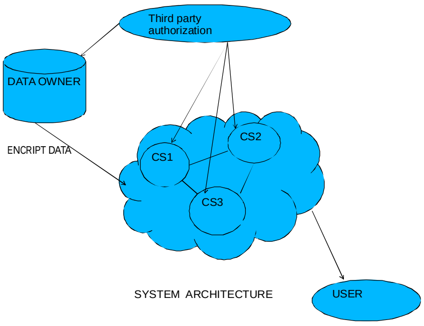


Fig1.SystemOverview

IV.SYSTEM OVERVIEW

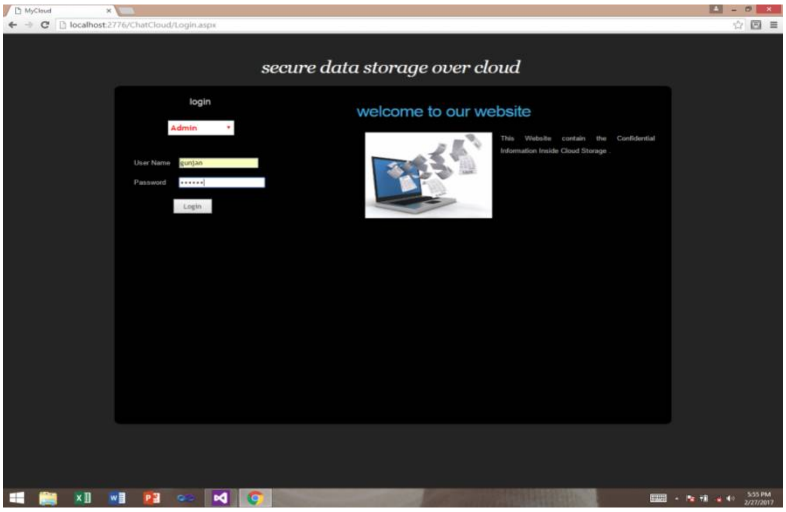
Verify Integrity Of Data Without Retrieve From Un-Trusted Server, This Helps In Realize Audit Service.
By Taking Requirement into Consideration We Can Achieve Privacy Preserving Public Auditing System for Cloud Storage .We Use One More Technique Bilinear Aggregate Signature to Handle Multiple Auditing. Bilinear Pairing Algorithm Is Better Auditing Algorithm Than Mac And Hla Algorithm. Bilinear Algorithm Provides Better Accuracy, Strong Encryption, Multiple UsersSetting. It Reduces Time Consumption, Increases Performance And Security.

V.METHODOLOGY

1. The organization admin first initializes the setup scheme using KEYGEN [11-12] algorithm to generate the keys and metadata and then sends them to the CSP.
2- The CSP replies to the request from the admin, by using the STNGEN [11-12] algorithm, to accept the set up Scheme. So, a connection initializes between the admin and the CSP. However, before outsourcing data to the CS, Data is encrypted by a powerful encryption technique called Advanced Encryption System (AES).
3- To achieve the information confidentiality, integrity, and availability, according to the CIA triad for the information Security, the user must have an account (Emails and password) to access stored data. In this system, more Restrictions upon these accounts are done by the admin to avoid data access by pre-activated accounts. Where, the Admin is the only one that can activate or not the accounts.
4- The activated users' accounts can login by using the two stages authentication technique; user name with password, And the TOTP that is permitted for one session between the user and the cloud server.
5- If the organization admin wants to audit the outsourced data on the cloud server, he resorts to the TP A who has The expertise to audit the data. However, the TP A must have an account in the system. This account must also Activate from the organization admin. If the TPA account is activated from the organization admin, then secret keand metadata would send to the TP A to audit the outsourced data on the CS, otherwise the TPA can't access the system.
6- TP A with the secret key and metadata sends the auditing request to the CSP to initialize the auditing process. 7- The CSP sends a query about the auditing process to the organization admin to authorize that query and TP A metadata by using the Automatic Protocol Blocker (APB).
8- If the APB is true, the admin sends the approval to the cloud service provider with the metadata; otherwise, the

VI.RESULTS

From our implementation and execution of our program we found that the mouse pointer can bemade to move and its functions can be implemented without the use of a touchpad or mouse .Thepointer is moved with the help of our finger gestures by placing the specific color substance inour hand (any colored cap or any colored small substance) making us easy to use our systemworks. The performance of the software has been improved.



localhost:2776/ChatCloud/Login.aspx

secure data storage over cloud

login

Admin

User Name: gunjan

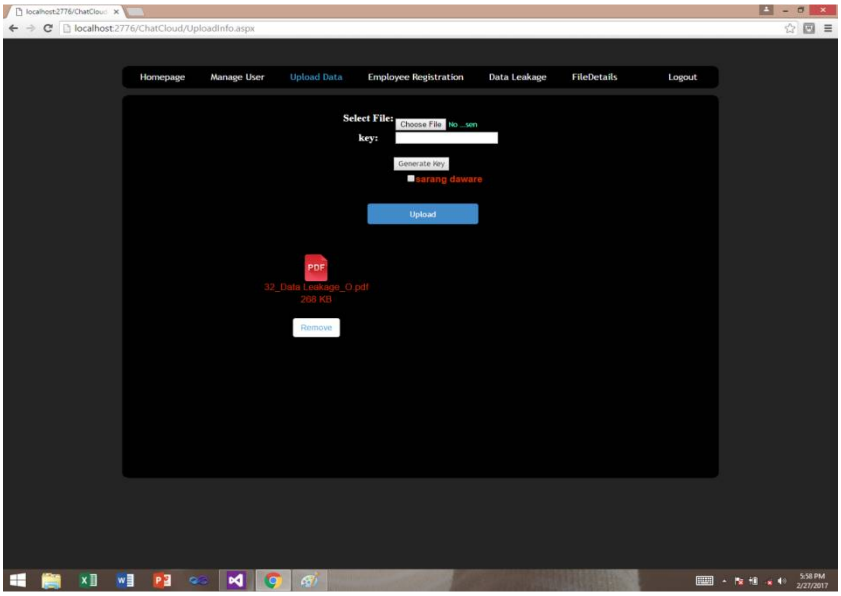
Password: ••••••

welcome to our website

This Website contain the Confidential Information Inside Cloud Storage .

Figure 1. Screenshot for mouse pointer functions in windows

As shown in figure 1. It shows the main application executable file on desktop which shows the login module for user , admin , third party named as less after opening the application we see the interface as shown in figure no 2.



localhost:2776/ChatCloud/UploadInfo.aspx

Select File: No ...sen

key:

□ sarang daware

32_Data Leakage_O.pdf
268 KB

Figure 2. Screenshot of mousless interagace.

The main window shows the image of generation of key and provide and provide the access to the admin for sending the data over the cloud .The file which send over cloud also provide the name and timing at which the file is send.

VII.CONCLUSION

In this project, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing, where TPA can perform the storage auditing without demanding the local copy of data. We utilize the homomorphic authenticator and random mask technique to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the ancient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing", Proceedings of Seventeenth IEEE InternationalWorkshop on Quality of Service (IWQoS'09), USA, pp. 1-9, 2009.

[2] A. Juels and B. S. Kaliski Jr., "Pors: proofs of retrievability for large files," Proceedings of the Fourteenth ACM Conference on Computer andCommunications Security (CCS'07), USA, pp. 584-597, 2007.

[3] H. Shacham and B. Waters, "Compact proofs of retrievability," Proceedings of the Fourteenth International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'08),LNCS, Berlin, pp. 90-107, 2008.

[4] M. Naor and G. N. Rothblum, "The complexity of online memory checking," Journal of the ACM, vol. 56, no. 1, pp. 2:1-2:46, 2009.

[5] E. C. Chang and J. Xu, "Remote integrity check with dishonest storage server," Proceedings of Thirteenth European Symposium on Research inComputer Security (ESORICS'08), LNCS, Spain, pp. 223-237, 2008.

[6] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proceedings of the Sixteenth ACM Conferenceon Computer and Communications Security (CCS'09), USA, pp.

[7] R. S. Kumarand A. Saxena, "Data Integrity Proofs in Cloud Storage," in Proceedings of the 3rd International Conference onCommunication Systems and Networks (COMSNETS'11), Bangalore, India, IEEE, 2011, pp. 1-4.

BIOGRAPHY

Mr R S Thakur Professor ,Department Of Computer Science And Engineering Of Dabasaheb Ambedkar College Of Engineering And Rerearch

Ms Ashwini Palghamol Researcher, Department Of Computer Science And Engineering Of Dabasaheb Ambedkar College Of Engineering And Rerearch
Area of interest Software Developer

Ms Devashri Gaikwad Researcher, Department Of Computer Science And Engineering Of Dabasaheb Ambedkar College Of Engineering And Rerearch
Area of interest Software Developer

Ms Gunjan Rakunde Researcher, Department Of Computer Science And Engineering Of Dabasaheb Ambedkar College Of Engineering And Rerearch
Area of interest Software Developer