International Journal of Data Mining Techniques and Applications
Volume 5, Issue 1, June 2016, Page No.74-75
ISSN: 2278-2419

Enabling Cloud Storage Auditing with Key Exposure Resistance

S.Santhiya[1], R. Arun[2]
[1]PG Scholar, [2] Assistant Professor
Department of ECE, Archana Institute of Technology, Sri Venkateswaraa College of Technology

Abstract - With cloud computing, users can remotely store their data into the cloud and use on-demand high-quality applications. Data outsourcing: users are relieved from the burden of data storage and maintenance When users put their data (of large size) on the cloud, the data integrity protection is challenging enabling public audit for cloud data storage security is important Users can ask an external audit party to check the integrity of their outsourced data. Purpose of developing data security for data possession at un-trusted cloud storage servers we are often limited by the resources at the cloud server as well as at the client. Given that the data sizes are large and are stored at remote servers, accessing the entire file can be expensive in input output costs to the storage server. Also transmitting the file across the network to the client can consume heavy bandwidths. Since growth in storage capacity has far outpaced the growth in data access as well as network bandwidth, accessing and transmitting the entire archive even occasionally greatly limits the scalability of the network resources. Furthermore, the input output to establish the data proof interferes with the on-demand bandwidth of the server used for normal storage and retrieving purpose. The Third Party Auditor is a respective person to manage the remote data in a global manner.

I. INTRODUCTION

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. From users' perspective, including both individuals and enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc . While these advantages of using clouds are unarguable, due to the opaqueness of the Cloud—as separate administrative entities, the internal operation details of cloud service providers (CSP) may not be known by cloud users—data outsourcing is also relinquishing user's ultimate control over the fate of their data.

II. PRIVACY-PRESERVING PUBLIC AUDITING

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).

Data Flow Diagram

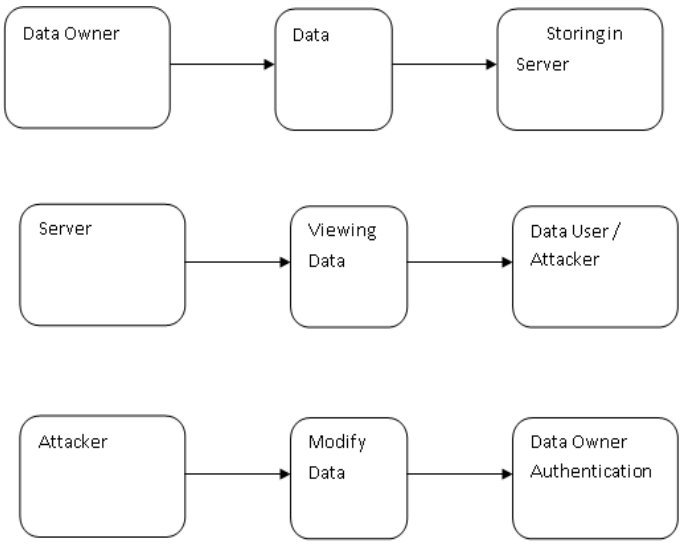

Figure 1: Data Flow Diagram

Use Case Diagram

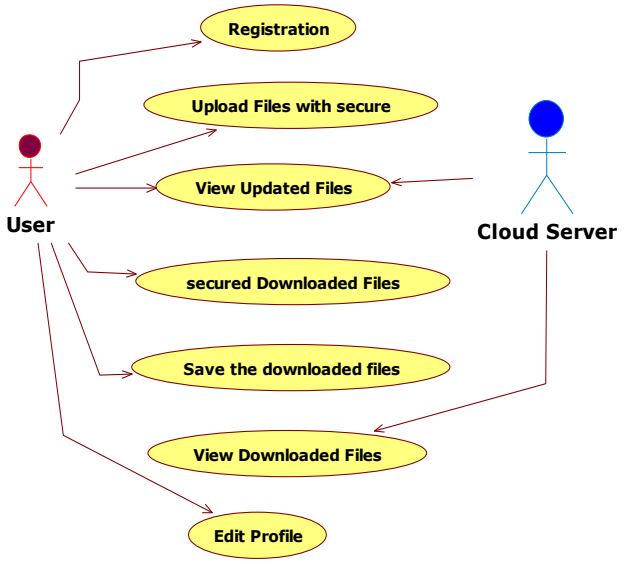

Figure 2: Use Case Diagram

International Journal of Data Mining Techniques and Applications
Volume 5, Issue 1, June 2016, Page No.74-75
ISSN: 2278-2419

Screen Shots

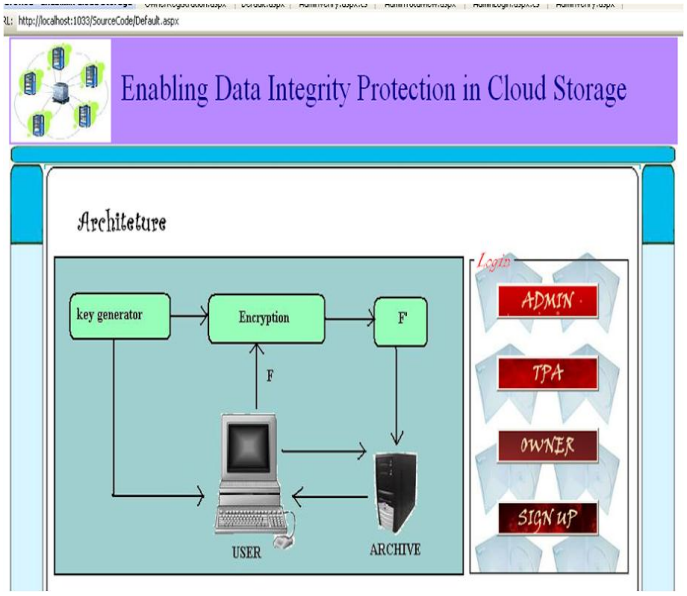

Figure 3: Main Page

Owner Login

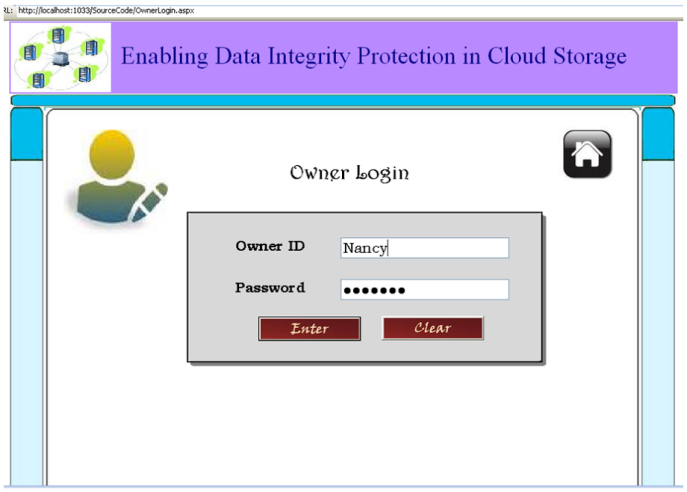

Figure 4: Owner Login

Secret Key Mail

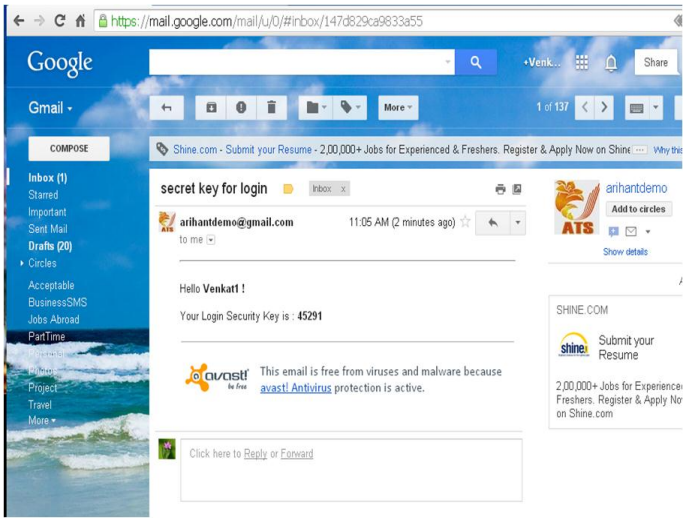

Figure 5: Secret key mail

Secret Key Login

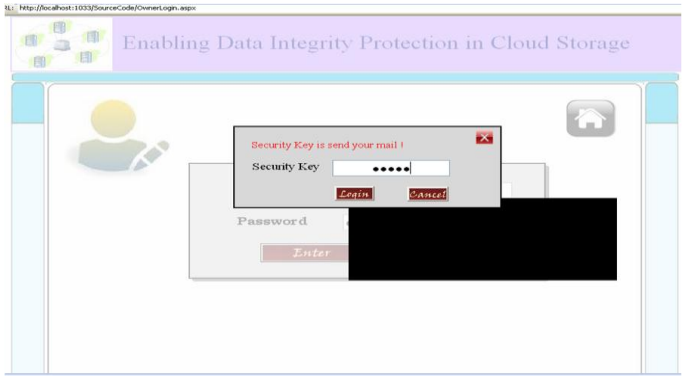

Figure 6 : Secret Key Login

File Upload

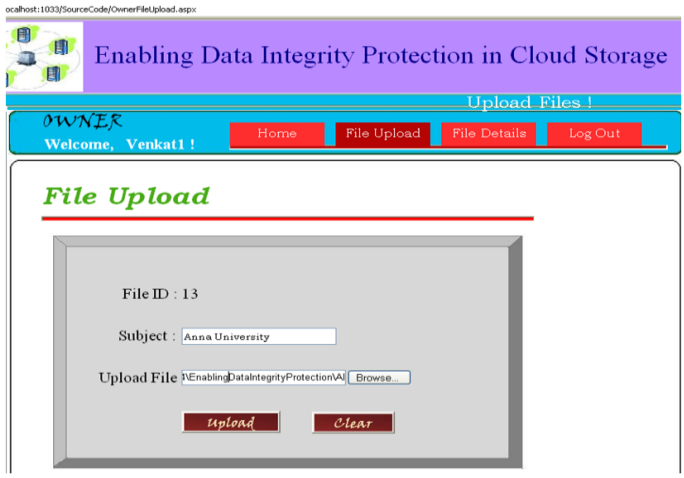

Figure 7: File Upload

III. CONCLUSION

We can further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient. We believe all these advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

References

[1] H. Abu-Libdeh, L. Princehouse, And H. Weatherspoon. Racs: A Case For Cloud Storage Diversity. In Proc. Of Acm Socc, 2010.
[2] R. Ahlswede, N. Cai, S.-Y. R. Li, And R.W. Yeung. Network Information Flow. Ieee Trans. On Information Theory, 46(4):1204–1216, Jul 2000.
[3] Amazon Elastic Compute Cloud. Http://Aws.Amazon.Com/Ec2/.
[4] Amazon Simple Storage Service. Http://Aws.Amazon.Com/S3/.
[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, And M. Zaharia. A View Of Cloud Computing. Communications Of The Acm, 53(4):50–58,