ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, *Volume 4, Special Issue 4, April 2015*

National Conference on Trends in Automotive Parts Systems and Applications (TAPSA-2015)

On 20th & 21st March

Organized by

Sri Krishna College of Engineering & Technology, Kuniamuthur, Coimbatore-641008, Tamilnadu, India

Secured Data Storage in Cloud Using Dynamic Auditing Protocol

Bala Brindha. M[1], Jeyakumari. M[2], Rajith Kumar.V [3]

P.G. Scholar, Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India[1]

ABSTRACT*:* Cloud computing has a promising pattern for data outsourcing and high quality data services. Some existing remote Integrity checking methods can only serve for statistic archive data and thus cannot be applied to the auditing service since the data in the cloud is dynamically updated and for verifying the integrity of an outsourced storage. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this project we first design an auditing framework for cloud storage systems and propose an efficient and privacy preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operation, which is efficient and probable secure in the random access model. We further extend our auditing protocol to support batch auditing for both multiple owners and clouds distributed over geographical area, without using any trusted organizer. The simulation and analysis results show that our proposed auditing protocols are secure, efficient and it reduce the computation cost of the auditor.

KEYWORDS: Dynamic auditing, privacy-preserving auditing, batch auditing, cloud computing.

I.INTRODUCTION

There are number of security issues associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers organizations using the services such as software, platform, or infrastructure as a service in cloud and the problems faced by their customers. Data integrity can be achieved using digital signatures and message authentication codes. It does not ensure availability, backup, and recovery are of little use. As the data gets produced, transferred, and stored at one or more remote storage servers, it becomes vulnerable. The third party auditing is important in creating an online service oriented economy, as it allows customers to evaluate the risks, and increases the efficiency of insurance based risk mitigation. Inspired by methods for auditing bricks and mortar businesses, we identify two approaches namely External Auditing and Internal Auditing. The public auditability for cloud storage is of critical importance so that users can use to a third party auditor (TPA) are used to check the integrity of outsourced data.Securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user is reduced and cloud storage system supporting privacy-preserving public auditing. Further extend result to enable the TPA to perform audits for multiple users simultaneously and efficiently. To significantly reduce the arbitrarily large communication overhead for public auditability without burden, we resort to the homomorphic authenticator technique.

II. SYSTEM DESCRIPTION

Modules:

Pre-computed challenging process

It supports public verifiability and privacy against third-party verifiers, while at the same time it doesn't need to use a third-party auditor. It is secure against the UN trusted server and private against third party verifiers.Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.

Data storage

An increasing number of clients store their important data in remote servers in the cloud, without leaving a copy in their local computers. It can be easily adapted to support data dynamics.

Owner Process

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 4, Special Issue 4, April 2015

National Conference on Trends in Automotive Parts Systems and Applications (TAPSA-2015)

On 20th & 21st March

Organized by

Sri Krishna College of Engineering & Technology, Kuniamuthur, Coimbatore-641008, Tamilnadu, India

The owner runs the key generation algorithm Key Gen to generate the secret hash key, the pair of secret-public tag key. Then, it runs the tag generation algorithm to compute the data tags. After all the data tags are generated, the owner sends each data component and its corresponding data tags to the server together with the set of parameters. The owner then sends the public tag key and the secret hash key and the abstract information of the data to the auditor, which includes the data identifier FID, the total number of data blocks n to the auditor.

Auditing Process

The auditor generates the challenge For all the data blocks in the data component and sends it to the server. Upon receiving the challenge C from the auditor, the server runs the prove algorithm Prove to generate the proof and sends it back to the auditor. When the auditor receives the proof from the server, it runs the verification algorithm Verify to check the correctness of P and extract the auditing result. The auditor then sends the auditing result to the owner. If the result is true, the owner is convinced that its data are correctly stored on the server, and it may choose to delete the local version of the data.

III. RESULT AND DISCUSSIONS

As a result of this implementation of dynamic auditing protocol for the encryption and decryption process the problems such as using the third party auditors for encrypting and decrypting the data was overcome and data's are uploaded and downloaded successfully. Dynamic auditing protocol works well and also supports for multiple user's. The results are shown in figures in step by steps

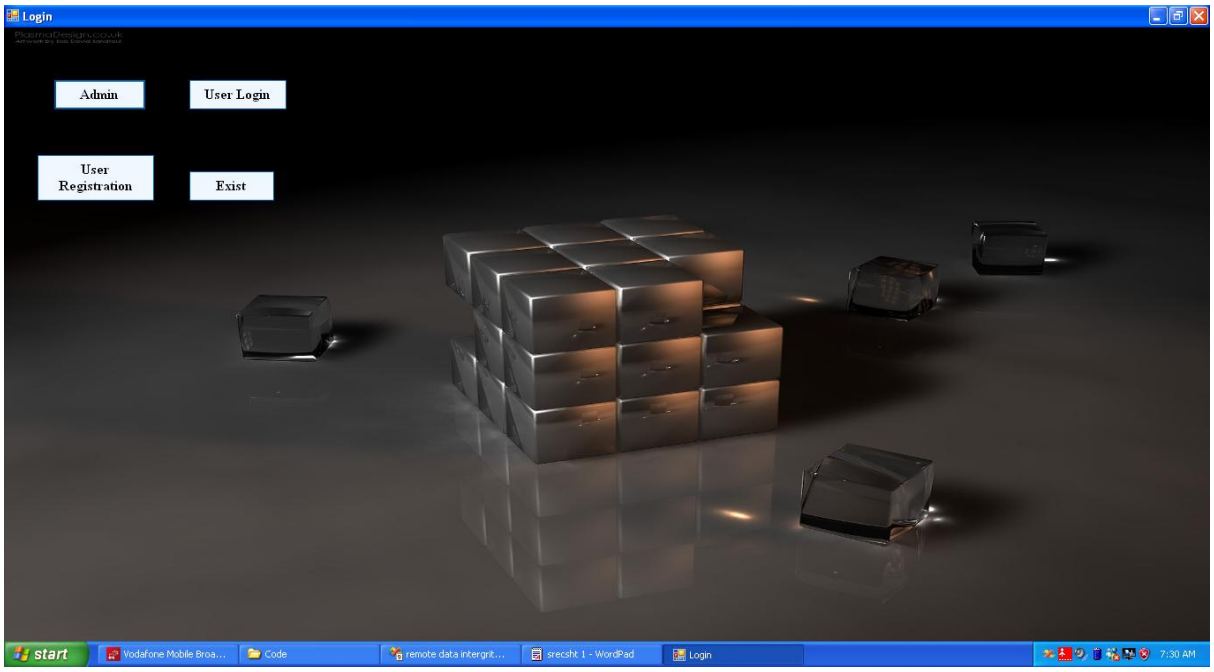

Figure 1: Login

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 4, Special Issue 4, April 2015

National Conference on Trends in Automotive Parts Systems and Applications (TAPSA-2015)

On 20th & 21st March

Organized by

Sri Krishna College of Engineering & Technology, Kuniamuthur, Coimbatore-641008, Tamilnadu, India

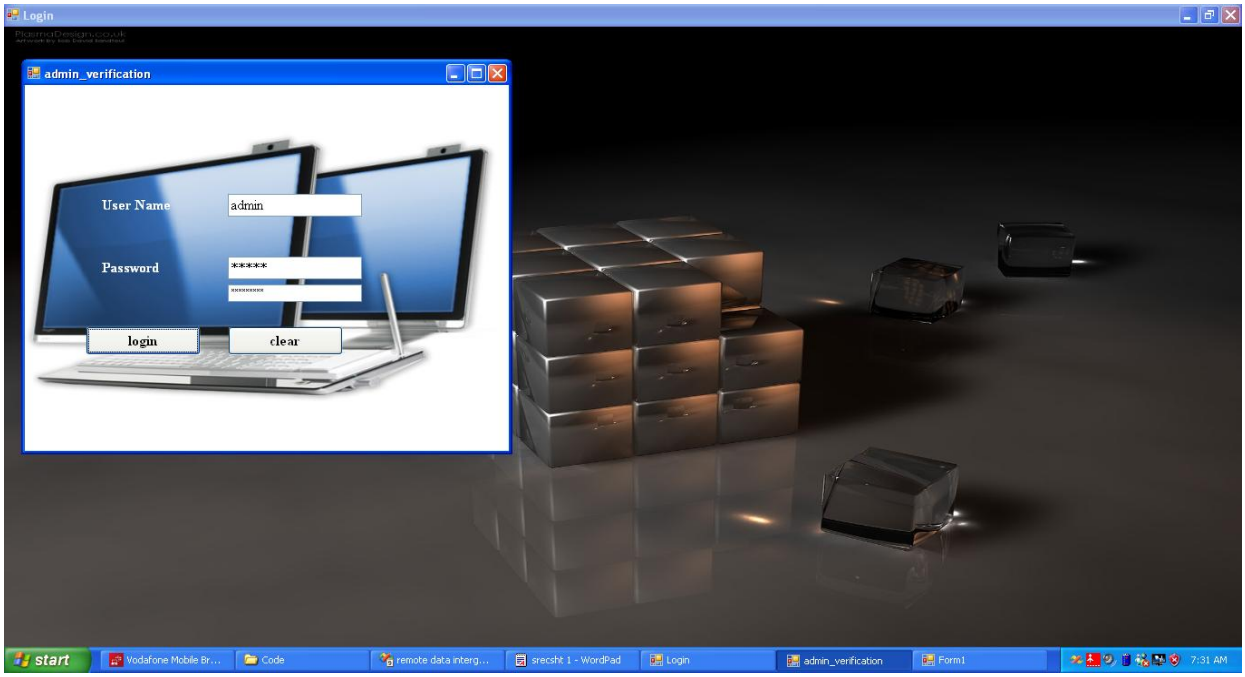

Figure 2: Admin login

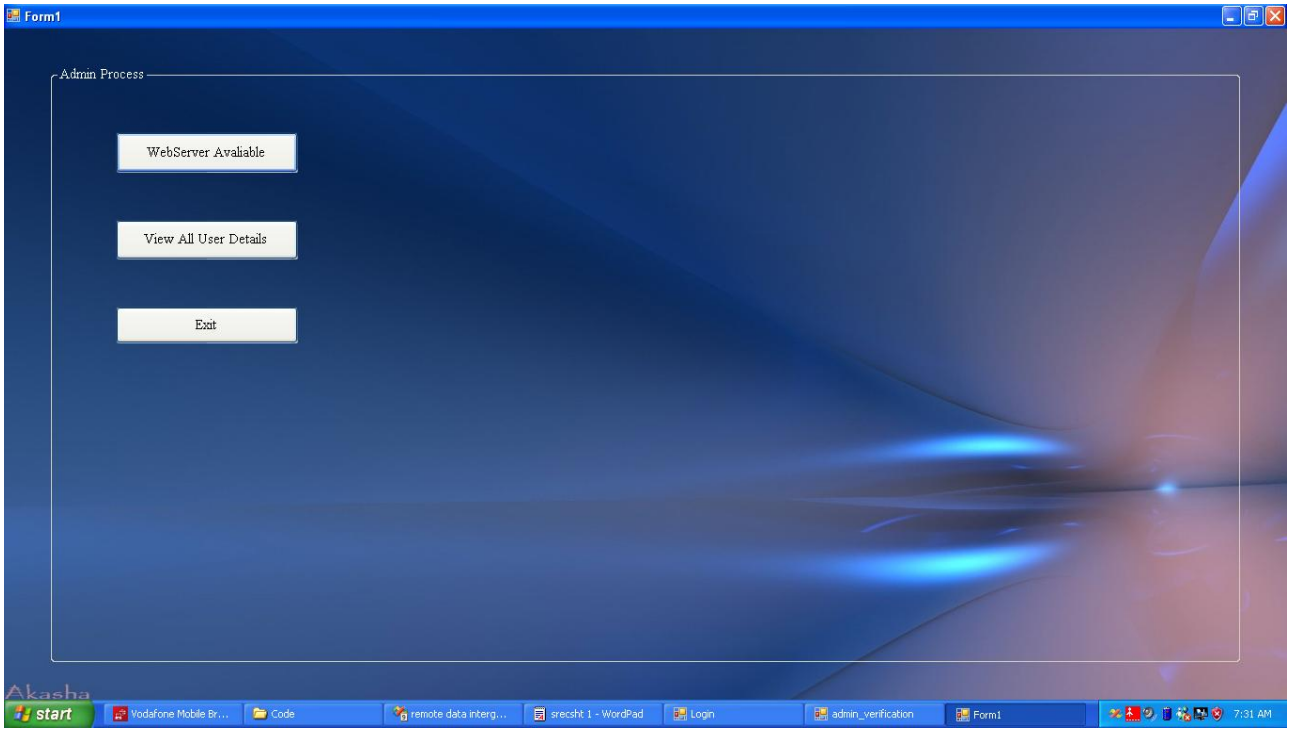

Figure 3: Admin process

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 4, Special Issue 4, April 2015

National Conference on Trends in Automotive Parts Systems and Applications (TAPSA-2015)

On 20th & 21st March

Organized by

Sri Krishna College of Engineering & Technology, Kuniamuthur, Coimbatore-641008, Tamilnadu, India

Figure 4: User page

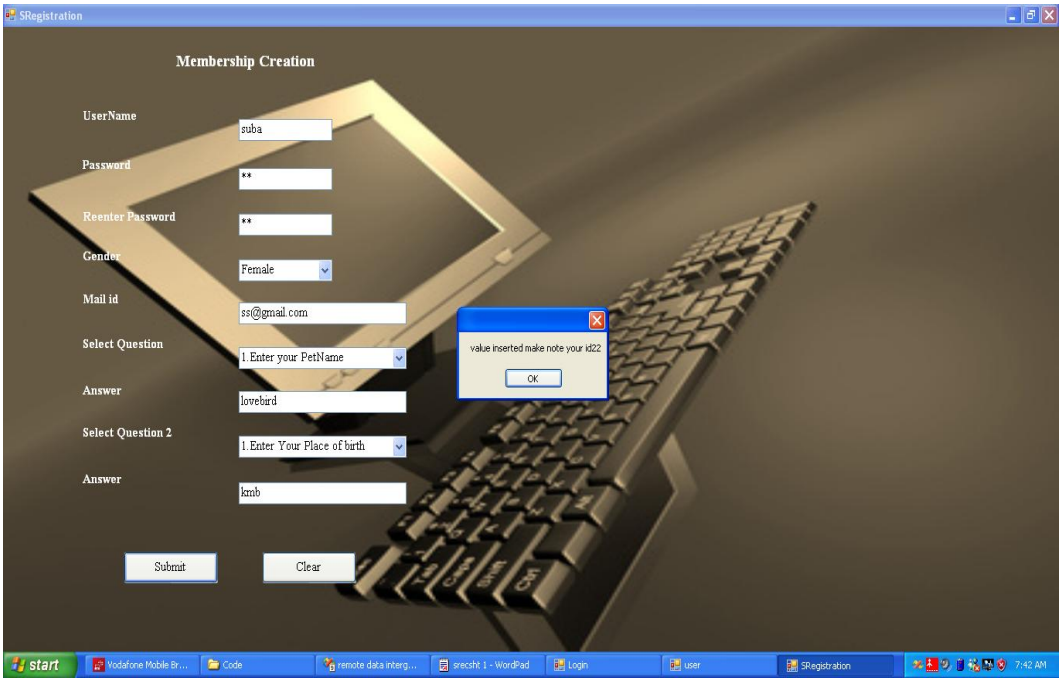

Figure 5: User membership creation

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, *Volume 4, Special Issue 4, April 2015*

National Conference on Trends in Automotive Parts Systems and Applications (TAPSA-2015)

On 20th & 21st March

Organized by

Sri Krishna College of Engineering & Technology, Kuniamuthur, Coimbatore-641008, Tamilnadu, India

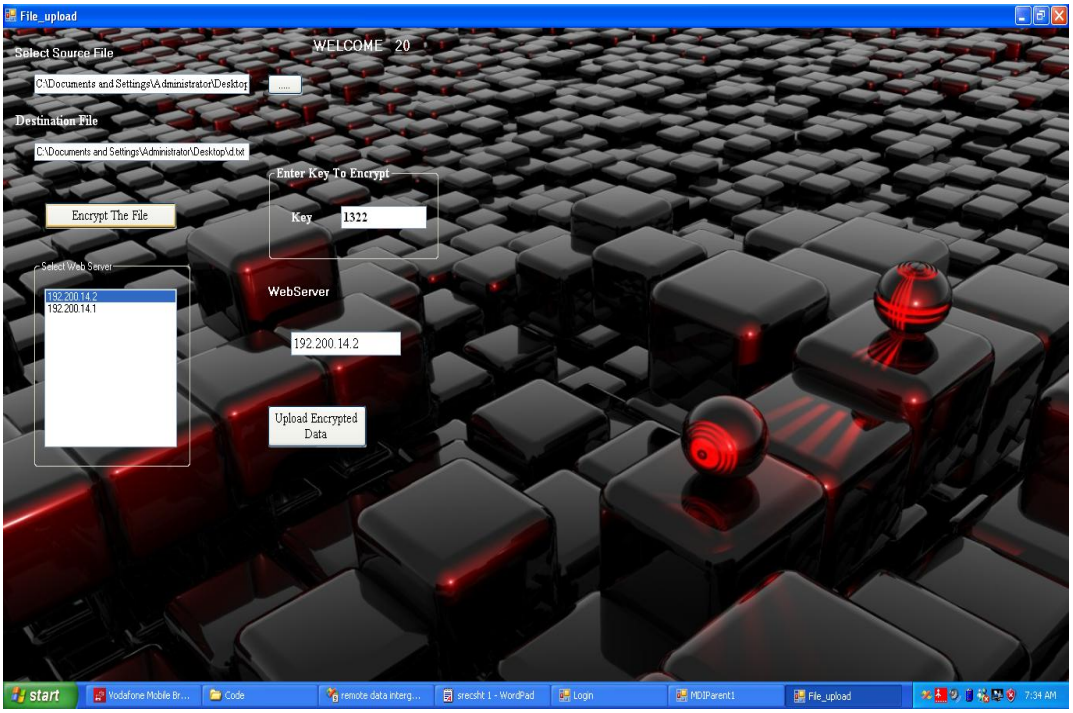

Figure 6: File upload

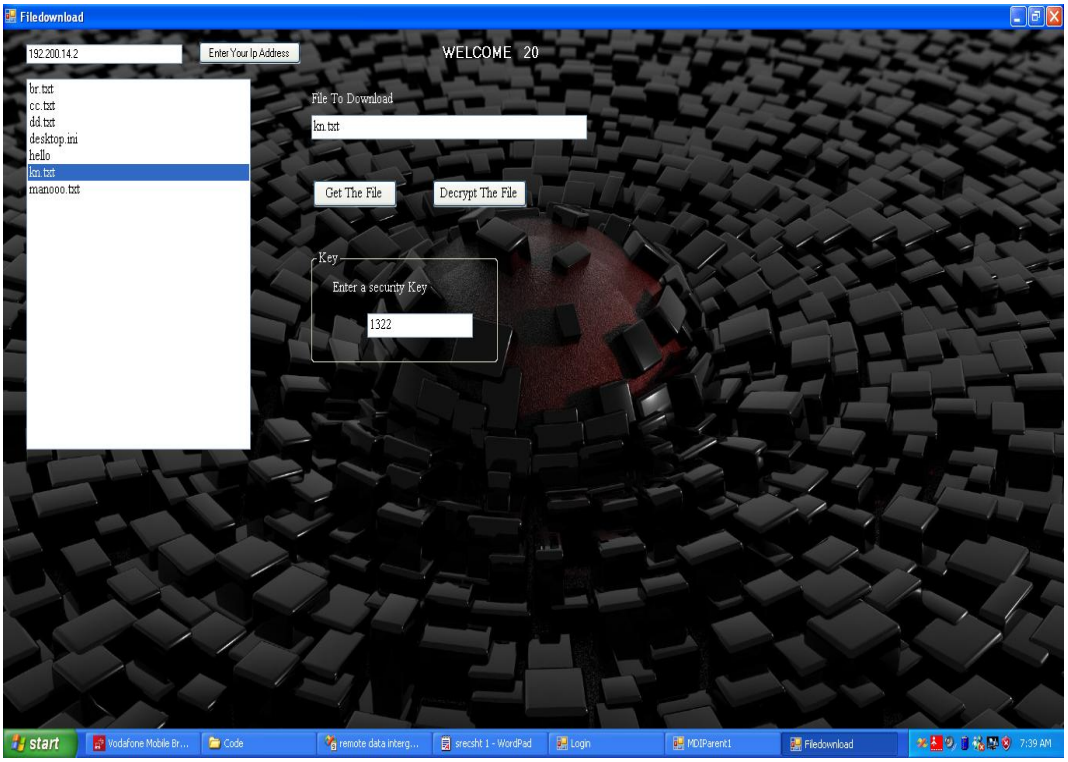

Figure 7: File Download

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, *Volume 4, Special Issue 4, April 2015*

National Conference on Trends in Automotive Parts Systems and Applications (TAPSA-2015)

On 20th & 21st March

Organized by

Sri Krishna College of Engineering & Technology, Kuniamuthur, Coimbatore-641008, Tamilnadu, India

IV. CONCLUSION

In this paper, we proposed an efficient and secure dynamic auditing protocol which protects the data privacy and the auditing process by combining the cryptography method with the bilinear paring, other than using the mask technique. The multi cloud batch auditing protocol does not require any additional organizer. The batch auditing protocol can also support the batch auditing for multiple owners. Furthermore, this auditing process incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server, this greatly improves the auditing process and also can be applied to big data on cloud storage systems.

REFERENCES

[1] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HOTOS), G.C. Hunt, ed., 2007.

[2] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[4] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.