JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enabling Storage Auditing In Cloud of Key Updates from Verifiable Outsource

Arjumand Fatima, Prof. S.D.Pingle.
People's Education Society's College of Engineering, Aurangabad, Maharashtra, India

Abstract: Key-introduction resistances have reliably an essential issue in various security applications. Recently the key exposure problem is proposed. The solution of key exposure problem is that client has to update his key in every time which is a new burden to the client. In our drawing, at the time of file uploading, knowledge owner can transfer a file in the cloud and Proxy server TPA simply has to hold a client's mystery answer whereas doing while doing all these burdensome tasks on behalf of the client. The client simply has to transfer the encoded mystery answer from the TPA whereas transferring new documents to the cloud to boot, our configuration likewise enhances the client with the capability to encourage settle for the legitimacy of the encoded mystery keys gave by the TPA. If TPA detects some corrupted files then it gets over the proxy server to examining system through key presentation resistance as easy as possible. The main objective of this paper is to make key transparent by updating keys, the key is updated by giving the time validity, and the validity is provided using the time server.

Keywords: Cloud data sharing, Key management, Security, efficiency..

1. INTRODUCTION

Cloud computing can help enterprises improve the creation and delivery of IT solutions by providing them with access to services in a cost-effective and flexible manner [1]. Clouds can be classified into three categories, depending on their accessibility restrictions and the deployment model. Cloud storage is one of the service provided by Cloud computing in which data is maintained, managed, backed up remotely and made available to users over a network. Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure. This gives you agility, global scale and durability, with anytime, anywhere data access. Cloud storage is purchased from a third party cloud vendor who owns and operates data storage capacity and delivers it over the Internet in a pay-as-you-go model. These cloud storage vendors manage capacity, security and durability to make data accessible to your applications all around the world. Data integrity is another part of cloud storage. Data integrity is a concept and process that ensures the accuracy, completeness, consistency, and validity of an organization's data. By following the process, organizations not only ensure the integrity of the data but guarantee they have accurate and correct data in their database. The importance of data integrity increases as data volumes continue to increase exponentially. Major organizations are becoming more reliant on data integration and the ability to accurately interpret information to predict consumer behavior, assess market activity, and mitigate potential data security risks. This is crucial to data mining, so data scientists can work with the right information. The user is concerned about the integrity of data stored in the cloud as the user's data can be attacked or modified by outside attacker. Therefore, a new concept called data auditing is introduced which check the integrity of data with the help of an entity called Third Party Auditor (TPA). The TPA performs the main role of data integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on it. It later compares both the signatures to verify whether the data stored on cloud is tampered or not. It verifies the integrity of data on demand of the users.

The key exposure problem, as another important problem in cloud storage auditing. The problem itself is non-trivial by nature. Once the client's secret key for storage auditing is exposed to cloud, the cloud is able to easily hide the data loss incidents for maintaining its reputation, even discard the client's data rarely accessed for saving the storage space. Cloud storage auditing protocol with key-exposure resilience by updating the user's secret keys periodically. In this way, the damage of key exposure in cloud storage auditing can be reduced. But it also brings in new local burdens for the client because the client has to execute the key update algorithm in each time period to make his secret key move forward. We show the system model for cloud storage auditing with verifiable outsourcing of key updates. There are three parties in the model: the client, the cloud and the third-party auditor (TPA). The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed, that is, the client can upload the growing files to cloud in different time points. This paper focus on how to make the key updates as transparent as possible for the client and propose a new scheme called cloud storage auditing with verifiable outsourcing of key updates. In this paper, Third party Auditor (TPA) is a trusted Authority to verify, audit and check update the file key on some period of time. For uploading file, client needs to send key request to the TPA. TPA will send encrypted secret key to the Client and using secret key client will encrypt file and store on cloud. This paper show that TPA plays two important roles, one is Audit the data file that is stored on cloud. And second is, update secret key of the client in each time period . In addition, TPA will audit whether the files in cloud are stored correctly or check the integrity of data by sending a challenge to cloud. In proposed scheme, key updates workload is outsourced to the TPA. Additionally this paper use the proxy server for save the file, when client uploads the file on the cloud automatically file saved on proxy server, if the file is hacked TPA will retrieve the file from proxy server.

2. EXISTING SYSTEM

Key-exposure resistance has always been an important issue for in-depth cyber defense in many security applications. To address the challenge, existing solutions all require the client to update his secret keys in every time period, which may inevitably bring in new local, burdens to the client, especially those with limited computation resources such as mobile phones. In existing system not provide the full security of cloud data. In this system, once the client's secret key for storage auditing is exposed to cloud, the cloud is able to easily hide the data loss incidents for maintaining its reputation, even discard the client's data rarely accessed for saving the storage space. In most of the previous systems, They propose a novel integrity auditing scheme for cloud data sharing services characterized by multi-user modification, public auditing, high error detection probability, efficient user revocation as well as practical computational/communication auditing performance.

3. ROPOSED SYSTEM

The system model for cloud storage auditing with verifiable outsourcing of key updates in Fig 3.1 There are three parties in the model: the client, the cloud and the third-party auditor (TPA). The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed, that is, the client can upload the growing files to cloud in different time points. The cloud stores the client's files and provides download service for the client. The TPA plays two important roles: the first is to audit the data files stored in cloud for the client; the second is to update the encrypted secret keys of the client in each time period. The TPA can be considered as a party with powerful computational capability or a service in another independent cloud. Similar to, the whole lifetime of the files stored in cloud is divided into T + 1 time periods (from 0-th to T -th time periods). Each file is assumed to be divided into multiple blocks. In order to simplify the description, do not furthermore divide each block into multiple sectors in the description of our protocol. In the end of each time period, the TPA updates the encrypted client's secret key for cloud storage auditing according to the next time period. But the public key keeps unchanged in the whole time periods. The client sends the key requirement to the TPA only when he wants to upload new files to cloud. And then the TPA sends the encrypted secret key to the client. After that, the client decrypts it to get his real secret key, generates authenticators for files, and uploads these files along with authenticators to cloud. In addition, the TPA will audit whether the files in cloud are stored correctly by a challenge-response protocol between it and the cloud at regular time. I have formalized the definition and the security model of the cloud storage auditing protocol with verifiable outsourcing of key updates. I am also going to prove the security of our protocol in the formalized security model and justify its performance by concrete implementation.

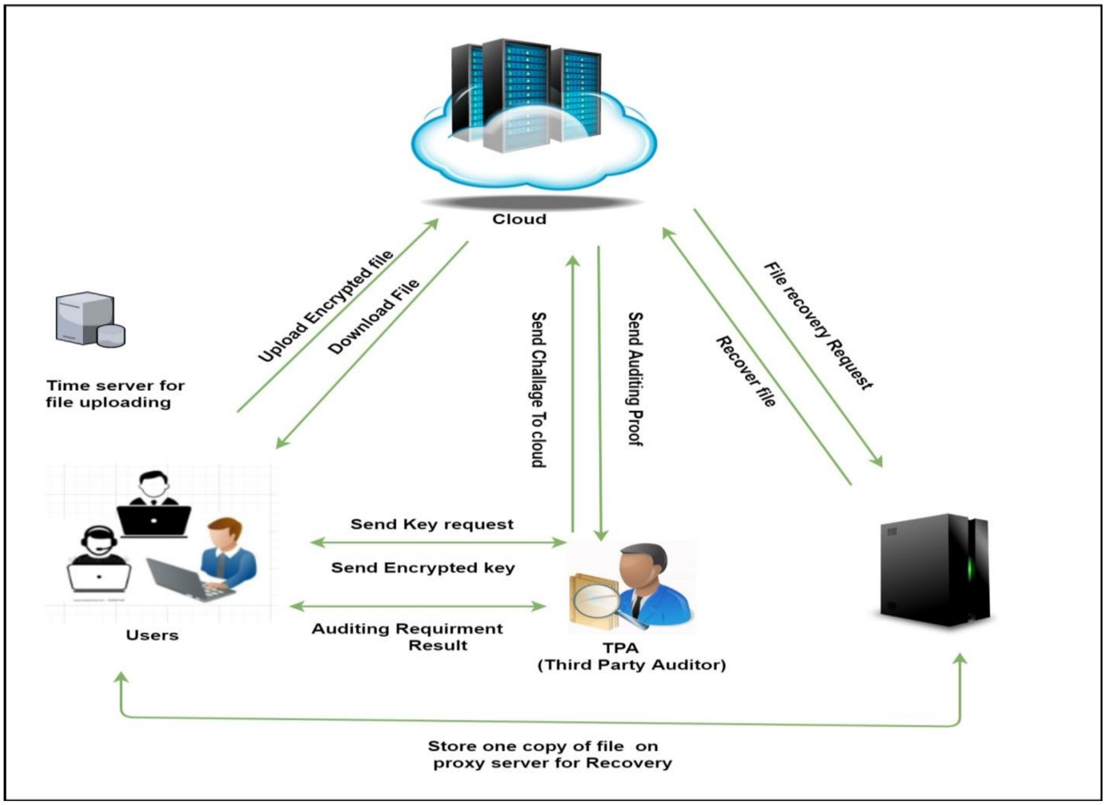


Fig1.0: System Architecture

4. Results & Screenshots:

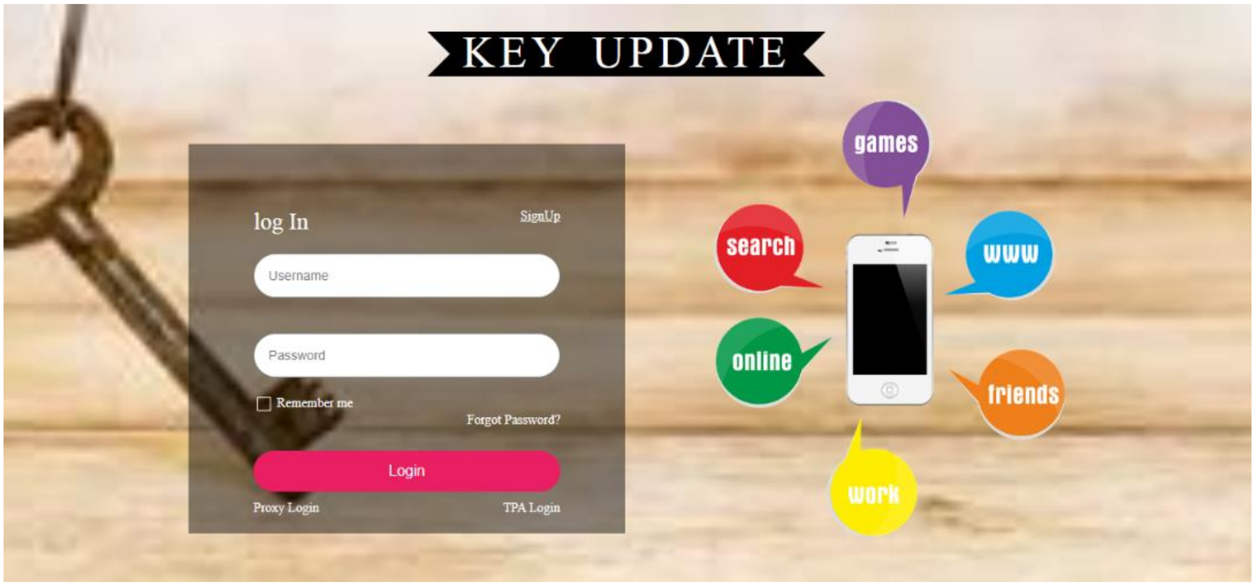


Fig.2: Login Page

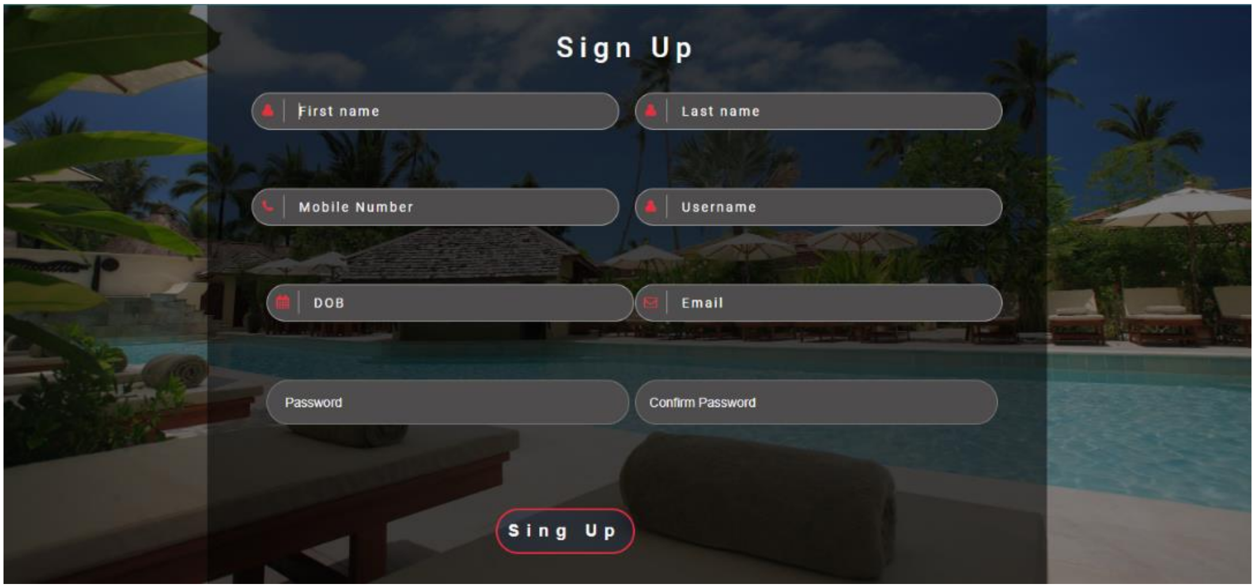


Fig 3. SignUp Page

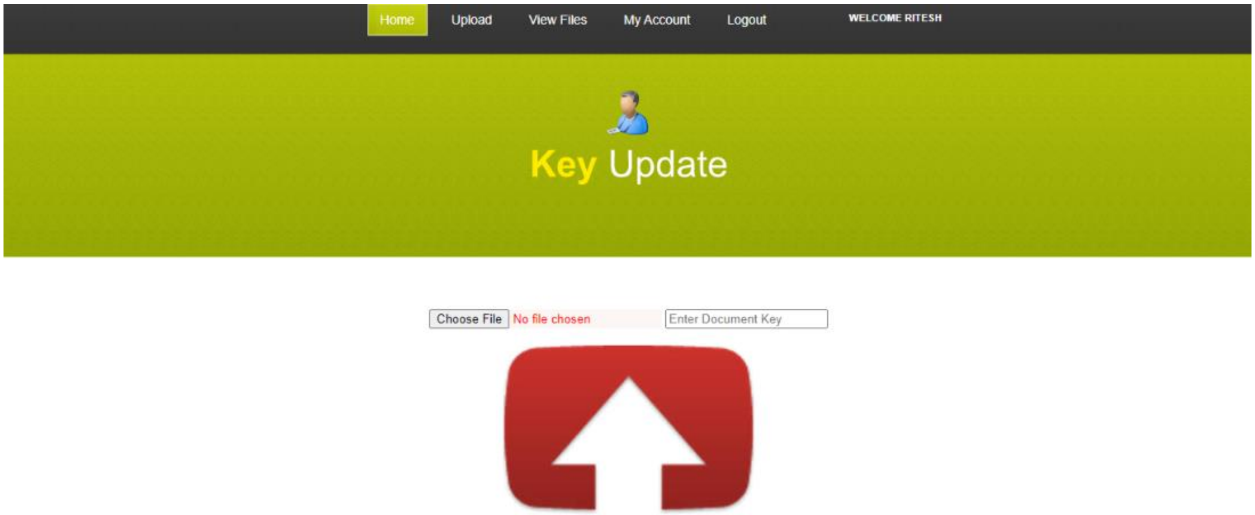
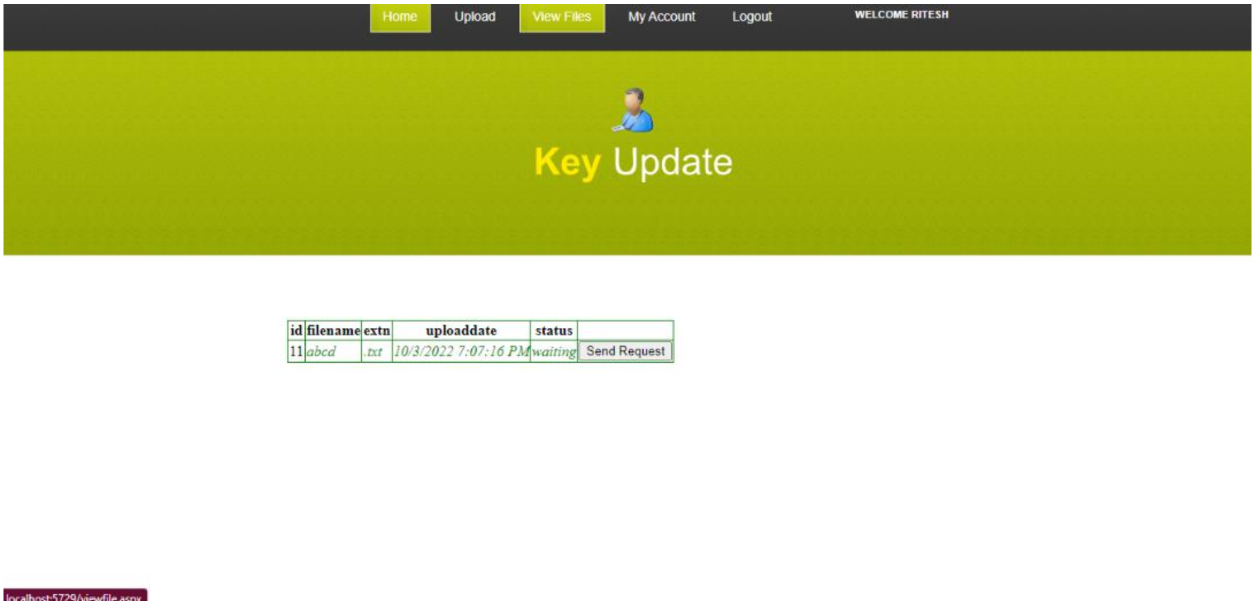


Fig.4. Upload File Page



id	filename	extn	uploaddate	status	
11	abcd	.txt	10/3/2022 7:07:16 PM	waiting	Send Request

Fig.5.View Upload Page

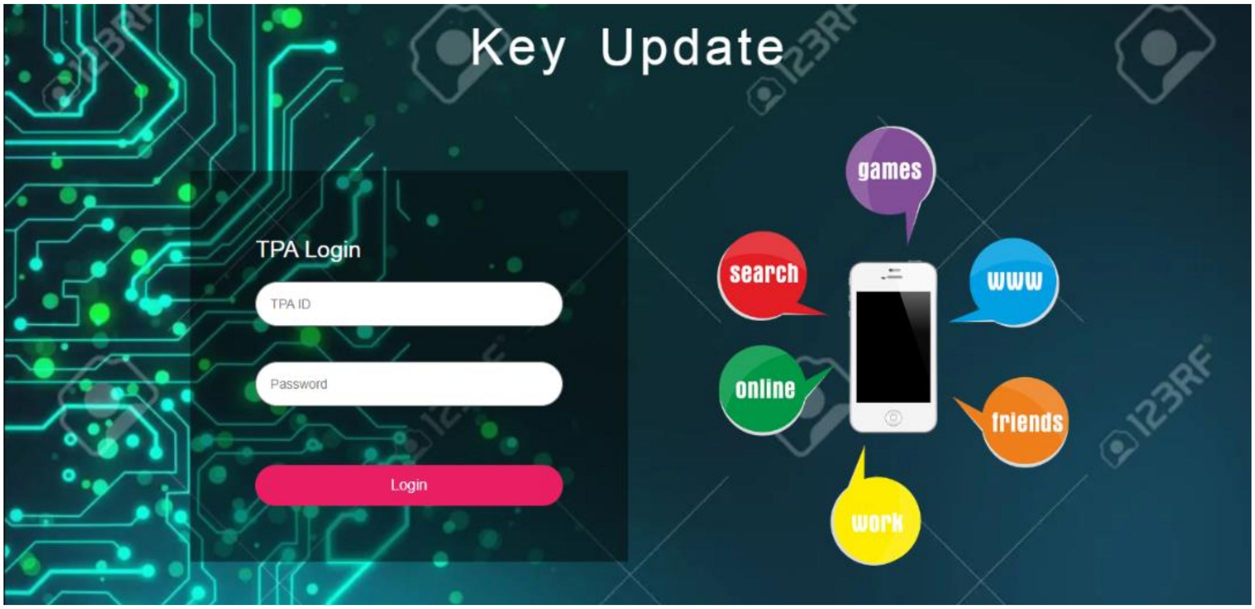
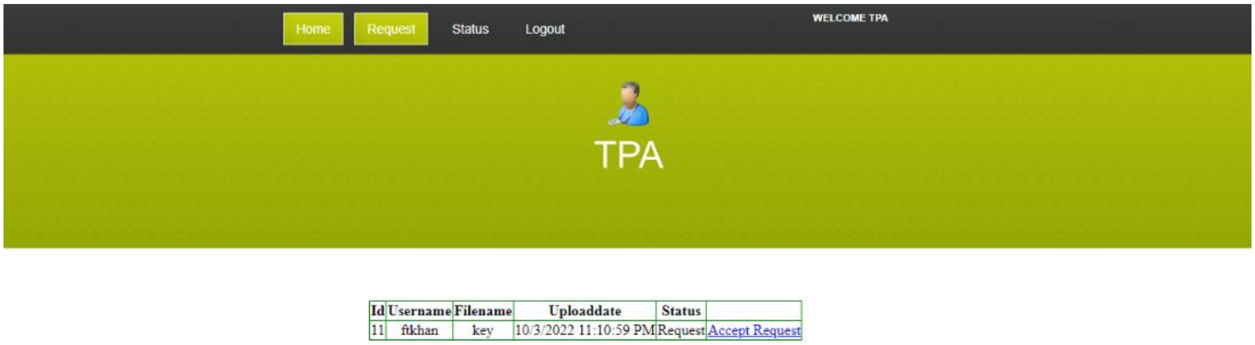


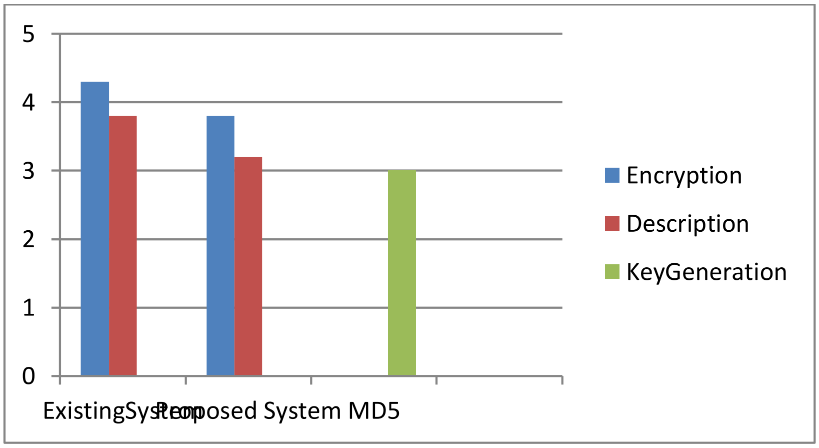
Fig.6. TPA Login Page



Id	Username	Filename	Uploaddate	Status	
11	ftkhan	key	10/3/2022 11:10:59 PM	Request	Accept Request

Fig.7: TPA Verification Page

5. Graphical Results:



The above graph shows the outcome result of proposed system. Result shows the time accuracy. The blue line shows the encryption timing in existing system, the red line shows the decryption time and the green color is for key generation. As per graph result shows that the existing system the time for encryption is 4.4sec and compare to that proposed system shows 3.8sec to encrypt the data. Whereas the decryption time is 3.8sec and 3.2sec in proposed system and the key update time is 3sec in proposed system so time is less in proposed system.

6. Conclusion:

I have Conclude that how to outsource key updates for cloud storage auditing through key exposure resilience. First I will propose cloud storage auditing protocol by verifiable outsourcing of key updates. In this protocol, key updates are out sourced to the TPA and are transparent for the client. In addition, the TPA only sees the encrypted version of the client’s secret key, as the client can further verify the validity of the encrypted secret keys when downloading them from the TPA. That offers the formal security proof and the performance simulation of the proposed scheme. And we used proxy server to recover file if auditing result fail. Then TPA recover file from proxy server and send result to the user..

7. REFERENCES:

[1] Cenamor, T. de la Rosa, S. N´u˜nez, and D. Borrajo, "Planning for tourism routes using social networks," Expert Systems with Applications, vol. 69, pp. 1–9, 2017.

[2] C. Yang, L. Bai, C. Zhang, Q. Yuan, and J. Han, "Bridging collaborative filtering and semi-supervised learning: A neural approach for poi recommendation," in Proceedings of the ACM SIGKDD Conference. ACM, 2017, pp. 1245–1254.

[3] Y. Liu, T.-A. N. Pham, G. Cong, and Q. Yuan, "An experimental evaluation of point-of-interest recommendation in location-based social networks," Proceedings of the VLDB Endowment, vol. 10, no. 10, pp. 1010–1021, 2017.

[4] H. Yin, W. Wang, H. Wang, L. Chen, and X. Zhou, "Spatial-aware hierarchical collaborative deep learning for poi recommendation," IEEE Transactions on Knowledge and Data Engineering, vol. 29, no. 11, pp. 2537–2551, 2017.

[5] Chua, L. Servillo, E. Marcheggiani, and A. V. Moere, "Mapping cilento: Using geotagged social media data to characterize tourist flows in southern italy," Tourism Management, vol. 57, pp. 295–310, 2016.

[6] G. Kim and L. Sigal, "Discovering collective narratives of theme parks from large collections of visitors' photo streams," in Proceedings of the ACM SIGKDD Conference, 2015, pp. 1899–1908.

[7] M. Versichele et al., "Pattern mining in tourist attraction visits through association rule learning on bluetooth tracking data: A case study of ghent, belgium," Tourism Management, vol. 44, pp. 67–81, 2014.

[8] J. Steenbruggen, E. Tranos, and P. Nijkamp, "Data from mobile phone operators: A tool for smarter cities?" Telecommunications Policy, vol. 39, no. 3-4, pp. 335–346, 2015.

[9] M. Culp and G. Michailidis, "An iterative algorithm for extending learners to a semi-supervised setting," Journal of Computational and Graphical Statistics, vol. 17, no. 3, pp. 545–571, 2008.

[10] C. Cortes and V. Vapnik, "Support vector machine," Machine learning, vol. 20, no. 3, pp. 273–297, 1995.

[11] Dean-Hall, C. L. A. Clarke, and J. Kamps, "Overview of the trec 2012 contextual suggestion track," in Proceedings of TREC, 2013.