13. The user now can upload the encrypted file to Storage Cloud.

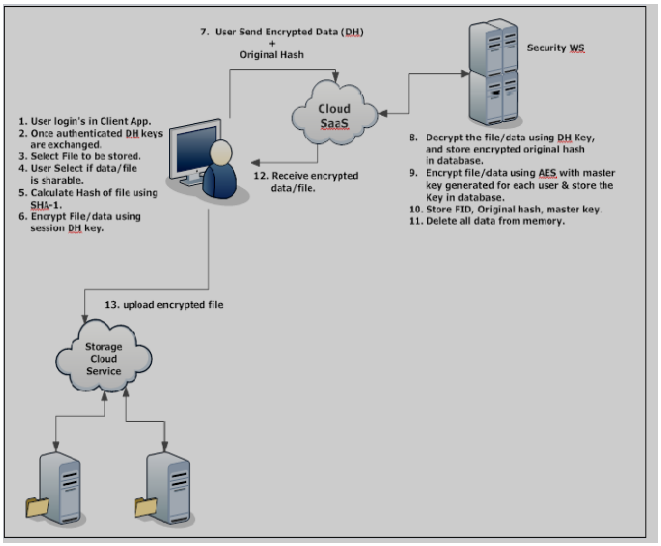


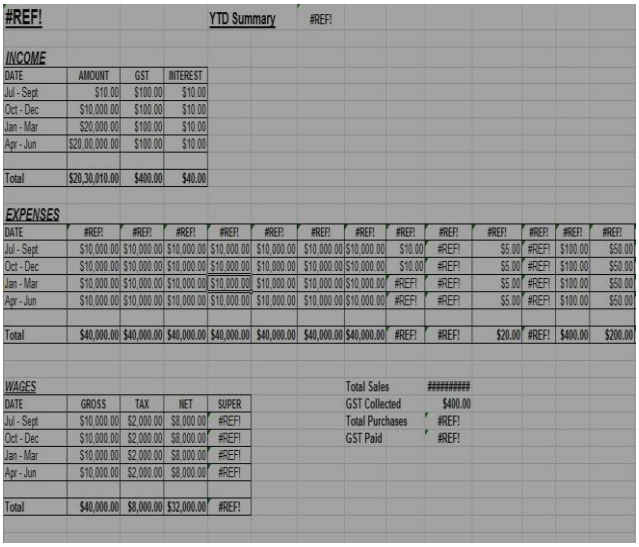
Figure 4.2: User Data Download Scenario

4.2 User Data Download Scenario

1) The end user login to the system with his/her username & password.
2) Once the user is authenticated, the Deffie Hellman key is exchanged for the session.
3) Now a user can select the files which he/she wants to download it from storage cloud.
4) The encrypted file is now downloaded from storage cloud to users match in.
5) The complete encrypted file is now transferred to Security Cloud.
6) The data in file is now encrypted using DH keys.
7) The complete encrypted file and original hash of file data are now transferred to Security Cloud.
8) At Security Cloud, decrypted files with Symmetric Algorithm namely AES using Master Key stored in security cloud database for each user.
9) The decrypted file is now encrypted with DH key.
10) The DH encrypted file and hash of the corresponding file is now passed to the users.
11) At user end, on receiving the encrypted file, it is decrypted with DH keys.
12) The hash of decrypted file is calculated using SHA-1 and original hash are now compared to see if they match, and accordingly appropriate message like, File tampered or File is intact are flashed on user screen. Thus the integrity of the data is verified.

5. Result Set

Let's take the example of "Yearly Tax Deduction" Excel File which we provide as an input to the system.



#REF! YTD Summary #REF!

INCOME

DATE	AMOUNT	GST	INTEREST
Jul - Sept	$10.00	$100.00	$10.00
Oct - Dec	$10,000.00	$100.00	$10.00
Jan - Mar	$20,000.00	$100.00	$10.00
Apr - Jun	$20,00,000.00	$100.00	$10.00
Total	$20,30,010.00	$400.00	$40.00

EXPENSES

DATE	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!	#REF!
Jul - Sept	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10.00	#REF!	$5.00	#REF!	$100.00	$50.00
Oct - Dec	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10.00	#REF!	$5.00	#REF!	$100.00	$50.00
Jan - Mar	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	#REF!	#REF!	$5.00	#REF!	$100.00	$50.00
Apr - Jun	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00	#REF!	#REF!	$5.00	#REF!	$100.00	$50.00
Total	$40,000.00	$40,000.00	$40,000.00	$40,000.00	$40,000.00	$40,000.00	$40,000.00	#REF!	#REF!	$20.00	#REF!	$400.00	$200.00

WAGES

DATE	GROSS	TAX	NET	SUPER
Jul - Sept	$10,000.00	$2,000.00	$8,000.00	#REF!
Oct - Dec	$10,000.00	$2,000.00	$8,000.00	#REF!
Jan - Mar	$10,000.00	$2,000.00	$8,000.00	#REF!
Apr - Jun	$10,000.00	$2,000.00	$8,000.00	#REF!
Total	$40,000.00	$8,000.00	$32,000.00	#REF!

Total Sales	#########
GST Collected	$400.00
Total Purchases	#REF!
GST Paid	#REF!

Figure 5.1: Sample Input

1. The file is exactly stored in encrypted format. The "userdata" in storage cloud is the table which stores the data for each user; Figure 8.2 shows the encrypted file which was stored by a user.

Figure 5.2: Encrypted Confidential File Stored In Storage Cloud

2. Secondly, the keys, hash of data are stored in security cloud server in "userkey" table, while the hash of corresponding data is stored in "filehash" table.

Format	Input	Output
Authentication	username/password dialog box	HTML Pages served after successful authentication
Query	Insert Command	Insertion of records
	Delete Command	One can also delete records inserted into the table
	Update Command	Modifying data already entered into the table

6. Conclusion

In this paper, a privacy-conserving public appraising mechanism for shared data in the cloud has been proposed. With this mechanism, the TPA is able to proficiently audit the integrity of shared data, yet cannot differentiate who is the signer on each block, which can maintain identity privacy for users. It offers user ambiguity in authentication phase, data integrity and confidentiality and the fair revocation process for all users. To improve the efficiency of verifying multiple auditing tasks, this mechanism supports batch auditing.

An interesting problem in future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

References

[1] Boyang Wang, Baochun Li and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE Transactions on Cloud Computing, Vol. 2, No. 1, 2014.
[2] Mohamed Nabeel and Elisa Bertino, "Privacy Preserving Delegated Access Control in Public Clouds", IEEE Transactions on Knowledge and Data Engineering, Vol. 26, No. 9, 2014
[3] Lukas Malina and Jan Hajny, "Efficient Security Solution for Privacy-PreservingCloud Services", 6th International Conference on Telecommunications Signal Processing Year 2013
[4] Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, 2014
[5] Yong Yu, Jianbing Ni, Man Ho Au, Yi Mu, Boyang Wang, and Hui Li, "On the Security of a Public Auditing Mechanism for Shared Cloud Data Service", IEEE Transactions on Services Computing, 2014
[6] Hong Liu, HuanshengNing, QingxuXiong, Member, Laurence T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 1, 2015
[7] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602-2614, Nov. 2013.
[8] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
[9] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227–238, 2013.
[10] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, doi: 10.1109/TSC.2013.2295611, 2013.
[11] I.T. Lien, Y.H. Lin, J.R. Shieh, and J.L. Wu, "A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for K-NN Search," IEEE Trans. Information Forensics and Security, vol. 8, no. 6, pp. 863-873, June 2013.
[12] A. Barsoum and A. Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 12, pp. 2375-2385, Dec. 2013.
[13] H.Y. Lin and W.G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, June 2012.
[14] J.Yu,P.Lu,G.Xue,andM.Li, "Towards Secure Multi-Keyword Top k Retrieval over Encrypted Cloud Data," IEEE Trans. Dependable and Secure Computing,vol.10, no.4, pp.239-250, July/Aug.2013.