Figure 6.13: User requesting For SK and Payment Details

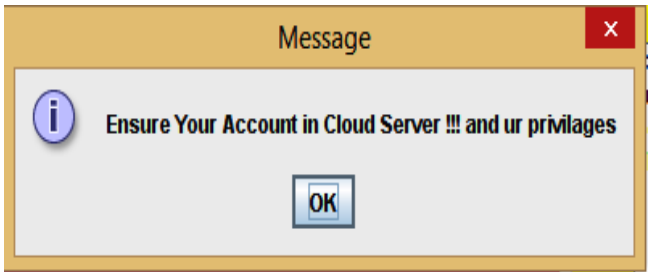

Figure 6.14: Message from TPA for denied-privileged access

7. Conclusion and Future Work

In this project, we have developed a system that solves the problem of data integrity, unauthorized access, privacy, consistency and also it aims for maintaining fine-grained data access control in cloud computing. This scheme presents a network in which cloud architecture, users, and TPA are shown, after that it describes retrieval of file, encryption and decryption of file, how to check the integrity of data from CSP and how to give control to TPA. Further, challenging issues for public auditing services that need to be focused. It is believed that security in cloud computing is very much needed as data in cloud storage are not secure. This project can be extended to incorporate efficient user revocation scheme.

References

[1] Josh Ames, http://blog.appcore.com/.
[2] http://www.cloud-competence-center.com/
[3] Neuman, C., and Ts'o, T. Kerberos: An authentication service for computer networks. IEEE Computer 32, 9 (September 1994).
[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peter-son, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609.
[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08. New York, NY, USA: ACM, 2008, pp. 1–10.
[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, Charleston, South Carolina, USA, 2009.
[7] Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.
[8] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of ASIACRYPT'08. Melbourne, Australia: Springer-Verlag, 2008, pp. 90–107.
[9] Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Cryptology ePrint Archive, Report 2008/432, 2008.
[10] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.
[11] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.
[12] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt 2003. Springer-Verlag, 2003.
[13] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT '04), Lecture Notes in Computer Science. Springer Verlag, 2004.
[14] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.
[15] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003.
[16] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, http: //seclab.cs.ucdavis.edu/projects/history/.
[17] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, March 2010.
[18] Kuyoro S. O., Ibikunle F. & Awodele O, Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011
[19] http://cloudtweaks.com/.
[20] Barrie Sosinsky, Cloud Computing Bible, Wiley India Pvt Ltd,2011.
[21] Greg Boss, Cloud Computing IBM 2007.10
[22] http://cloudtweaks.com/.
[23] Greg Boss, Cloud Computing IBM 2007.10