Abstract

Cloud computing provides remote users a flexible and convenient way to obtain cloud services on demand such as cloud storage service, which has been facing great security and privacy challenges, especially insider attacks. However, most of the previous work on the cloud security focusing on the storage security can't be effective against insider threats. Wei's scheme on the cloud storage, which is based on an ID-based strong designated verifier signature (IBSDVS) protocol, takes privacy and confidentiality into consideration. But it also can't be against insider attacks and its confidentiality exists security flaws. Hence, in this paper, we propose an efficient data storage protocol in the cloud computing, which can be against insider attacks as well as providing privacy preserving and confidentiality. Similar to Wei’s scheme, our protocol adopts an IBSDVS scheme that has the secure property of non-delegatability. Then the analysis of security and performance are described in detail.

References
19. D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” in
Advances in Cryptology\textdagger


24. P. Golle and I. Mironov, “Uncheatable distributed computations,” in Topics in Cryptology\textdagger


\textbf{Index Terms}

\begin{tabular}{ll}
Computer Science & Security
\end{tabular}
Keywords

Cloud computing, storage security, designate verifier signature, privacy preserving, and insider attack.