Abstract
In this century all personal data are stored on cloud or on servers such as passwords, account numbers, notes, and other important information, but there is chance of misusing people's saved data by a competitor, a miscreant, a court of law. Confidentiality, Integrity and Availability (CIA) are the big challenges related with data storage management. Sometimes, the cloud service providers store or cache the personal information without user's authorization or permission and control. To prevent this, a self-destructing data system providing user's data security is used. In self-destructing data system, all the data stored on cloud or on servers are destructed automatically or transform into an unreadable state after the user specified time, without the user's intervention. In this paper, SeDas: self-destructing system for data security which is based on integration of cryptographic techniques is presented. Here a proof-of-concept of SeDas prototype is executed. Through the functionalities and properties of SeDas prototype, SeDas is proved to preserve all the data privacy and also it can be practically used. Output of downloading and uploading with SeDas system decreases and latency increases as compared to the system without self-destructing data mechanism. In this paper, different data security techniques are compared.

References

- L. Qin and D. Feng, &quot;Active storage framework for object-based storage device,&quot; in Proc. IEEE 20th Int. Conf. Advanced Information Networking and Applications (AINA), 2006.
- Y. Zhang and D. Feng, &quot;An active storage system for high performance computing,&quot; in Proc. 22nd Int. Conf. Advanced Information Networking and Applications (AINA), 2008, pp. 644–651.

Review: The Secret Sharing Algorithms for Data Security in the Cloud


Index Terms

Computer Science

Security

Keywords

Secret Sharing Data Security Symmetric Encryption