Abstract

Presently technical and legal landscape presents formidable challenges in data privacy. The personal data’s like password, account number and any other important information’s are cached, copied and achieved by the service providers. destroying of data mainly aims at providing data privacy. The data is deleted after the specified time i.e., the decryption key is deleted so that after the specified time the data cannot be accessed by any, in other words the data is deleted. Our research seeks to protect the privacy of past, archived
data such as copies of emails maintained by an email provider against accidental, malicious, and legal attacks. In this paper we provide a back up copy of a data is kept in a local system when the data is destructed in the cloud. and also in our research we provide a one time password for the first login. Specifially, we wish to ensure that all copies of certain data deleted after a user specified time, without any specified action on the part of a user, and even if an attacker obtains both a cached copy of that data and the user's cryptographic keys and password.

References

- Poettering, 2006, SSSS: Shamir and Secret Sharing Scheme [Online].
Privacy Protection of Data in Cloud by Destroying Data at Predefined Time


Index Terms
Keywords
Data Privacy  Self Destructing  Cryptographic Keys And Password