Outsourcing Data Sharing Requirements to an Untrusted Service Provider

Ravi Chandra Jammalamadaka, Sharad Mehrotra
Donald Bren School of Information and Computer Sciences
University of California, Irvine, CA 92697, USA
$\{rjammala, sharad\}@ics.uci.edu$

I. Abstract

Mechanisms for data sharing are a fundamental need for both individuals and organizations. With the proliferation of networking technologies and multimedia devices, end users are generating a lot of personal information such as email, pictures, video albums, etc. Users share their personal information using a variety of methods such as disseminating information via email, posting data on a publicly accessible websites, etc. Such solutions have severe security drawbacks as authorized recipients can gain access to personal data. Expecting users to install and administer data sharing architectures is unrealistic and infeasible. Likewise, organizations require trained professionals, hardware and software infrastructure to put in place a secure data sharing architecture, making it cost-expensive solution.

Recently, there are emerging solutions which allow users/organizations to outsource their information to a third party. The third party is now entrusted with the task of providing data management tasks which includes enforcing data sharing requirements. For instance, Yahoo! Briefcase and Apple's Idisk are examples of such services. These services provide the user with storage space and some preliminary data sharing functionality. Advantages of such services include a) Availability: The data can be accessed 24/7 at an Internet scale; b) Less cost: The service provider can amortize the cost over several clients; and c) Better service: The service providers typically employ experts to provide better quality service.

The primary limitation of such services is the requirement of *trust* on the service provider. The User's data is stored in plaintext and therefore is susceptible for the following attacks: a) Outsider attacks: There is always a possibility of Internet thieves/hackers breaking into the service provider's system and stealing/corrupting user's data; and b) Insider attacks: malignant employees of the service provider can steal the data themselves and profit from it. There is no guarantee that client's data confidentiality and data integrity are preserved at the server side.

In this work we are exploring techniques which allow individuals and organizations to outsource their sharing requirements to an untrusted service provider. To preserve data confidentiality of the client, encryption offers a natural solution. The user's data can be encrypted before being outsourced to the server. When access to the data is required, the appropriate data can be fetched from the server and decrypted at trusted user location. The objective now is to provide the data sharing services over encrypted data. There are many challenges that need to be addressed before a data sharing architecture of this kind can be realized. They are: a) capturing user's security policy; and b) enforcing the user's security policy via cryptographic techniques in a dynamic setting. Information belonging to the user is always accompanied by a sharing policy. The security policies could range from *share-everything* to *share-nothing*. The user will desire complete control in allowing other users either a partial or complete view of his/her information. Development of a policy language is the key, which will dictate the sharing semantics. After a language is built that captures the security policy of the user, mechanisms should be in place that enforce the security policy. There are many challenges that need to be addressed before the security policy can be enforced at the service provider: a) Authentication of users should be now take place at the service provider b) Access control should now take place at the service provider over encrypted data. The problems are further compounded with the fact that sharing policies/requirements are dynamic in nature.

In summary, we are exploring techniques/mechanisms that allow an untrusted service provider to provide data sharing services to individuals or organizations, while preserving security properties such as data confidentiality and integrity of the client. We have identified some of the challenges that need to be addressed in an architecture of this kind and these challenges form the basis of our future work.