Secure Data Sharing with Controlled Access to User

by

Ahmed Shaik

A thesis for Master submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Computer Engineering

Program of Study Committee:
Yong Guan, Major Professor
Diane Rover
Doug Jacobson

Iowa State University

Ames, Iowa

2017

ABSTRACT

The rapid adaptation of mobile devices and data sharing has changed our life style significantly. Despite the fact that this provides extraordinary comfort and proficiency, they also impose greater challenges in ensuring a secure transfer of sensitive information through these devices. This information could be highly confidential that the owner wants to provide access privileges only to authorized individuals. Many cryptographic algorithms together with potent data protection mechanisms available today are robust enough to ensure the Confidentiality, Integrity and Availability of information. One significant use-case in this regard is when the data owner only wants to share the data securely with the authorized user, without providing him/her the privileges to store or make a copy of the data or to share it with others. In this scenario, it is practically impossible for the data owner to be available and spy on the user all the time to ensure these security requirements are met.

In order to address this concern, in this thesis work, a new and secure mechanism to share information is introduced that would authorize end users to access data only a certain number of times as decided by the data owner, and prevents the user from duplicating the data and sharing it with unauthorized users. A part of this work proposes a variant of Proxy Re-encryption algorithm, a relatively new cryptographic primitive, which offers the data owner a way to securely share his data via a proxy server, without the need to be available all the time. The proxy server takes care of data re-encryption and data distribution to the registered users, without letting any unauthorized user or the proxy itself to decrypt the information. With this scheme, the proxy modifies an already encrypted information in such a way that another secret key can decrypt it. The proxy server has access only to the original cipher text and re-encryption keys, both of which are provided by the data owner and are available publicly at all the times. The re-encryption key is unique for each registered users and is generated by the data owner by combining the receiver's public key and his own private key. Now, the novelty of this thesis and most challenging part is to prevent the user from storing the decrypted data or making a copy of it. To meet these security requirements, in this research work, the proxy re-encryption algorithm is finely tweaked, along with a novel way of leveraging the security features of recipient's device (iOS). Using the unique variant of proxy re-encryption and exploiting the security features of an iOS device to restrict the receiver from storing or duplicating the sensitive information transferred, is the core essence of this thesis work.

The experimental evaluation and results displayed that the proposed scheme can be effectively used to share sensitive data with authorized users while preventing the users from sharing with unauthorized users. The results also show that the time taken for each query to display a block of data is only slightly increased with the addition of this scheme and almost negligible, proving that the proposed scheme doesn't add significant latency to the original proxy re-encryption algorithm.