MASTER'S PROJECT (Fall 2013)

TOPIC: ***Securing Critical Data in Cloud Using Multiple Digital Signatures***

PRESENTOR: Chang Wei Huang

ADVISOR: Dr. Haiping Xu

DATE & TIME: Friday, October 25 2013, 3:15 PM

LOCATION: Dion 101

COMMITTEE MEMBERS: Dr. Shelley Zhang and Dr. Firas Khatib

ABSTRACT

Cloud computing allows users to store data into the cloud and manage it all around the world. Due to the much reduced cost of hardware and software maintenance using cloud services, storing data in cloud has become a common trend for modern users. Despite the popularity of cloud services, data security has become a major concern when cloud storage is used, especially for critical and sensitive data such as medical records of patients. In this project, we propose to use multiple digital signatures to secure critical data stored in cloud. The approach can be used to authenticate the identities of multiple signers of a document, and to ensure that the original content of the document is not changed in cloud. As a major verification approach, digital signature employs a type of asymmetric cryptography, which has the following properties: 1) non-repudiation: the signer cannot deny his/her signature afterwards; 2) integrity: a user cannot forge a signer's signature, and any change in the document after it is signed will invalidate the signature; 3) authentication: a user can verify that a digital signature is indeed given by a legitimate signer. The digital signature approach is based on the public key encryption technology, where each signer generates his/her public-private key pair. The signer keeps the private key that is used to generate a digital signature for a give document, and the digital signature can then be verified using the public key. To demonstrate the usability and effectiveness of our approach, we adopted a case study in healthcare, and developed a prototype system for mulitple users to digitally sign medical documents, and upload or download them at cloud storage. The prototype system is implemented in Java and is powered by Google App Engine and RESTful web services.