Chapter 36
Cloud Computing Data Storage Security Based on Different Encryption Schemes

Hicham Hamidine
University of Bridgeport, USA

Ausif Mahmood
University of Bridgeport, USA

ABSTRACT

Cloud Computing (CC) became one of the prominent solutions that organizations do consider to minimize and lean their information technology infrastructure cost by fully utilizing their resources. However, with all the benefits that CC promises, there are many security issues that discourage clients from making the necessary decision to easily embrace the cloud. To encourage the use of CC, clients need to be able to strategically plan their future investments without the uncertainties of security issues that come with hosting their data in the cloud. This chapter will discuss different mitigation techniques and the common proposed security algorithm schemes for data storage encryption based on classical "symmetric and asymmetric" and with an emphasis on fully homomorphic encryption schemes.

INTRODUCTION

Globalization has forced organizations to accomplish a lot with far less technical, personnel and budget resources. Therefore, when the cloud model was introduced and started to mature it became an obvious choice to many corporations regardless of size. This new model promises that clients can have as many hardware, and software resources as they wish and when it's most needed, which made scalability an issue of the past and at a much less cost. Today, most of the cloud services are in the nature of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services revolutionized the way information technology decision makers assess projects and their related risks versus return on investments. However, the looming security risks and issues an organization may face

DOI: 10.4018/978-1-5225-8176-5.ch036

still are the biggest obstacles that refrain clients from fully harnessing the benefits of the cloud; especially for those whom their data security is an essential component of their daily business.

Many solutions have been identified to achieve security in the cloud and protect data either by using access control, data storage encryption, or a combination of the two. This paper presents a comprehensive survey of different encryption schemes used or are proposed to protect data in the cloud including the algorithm(s) the scheme uses to achieve the sought after level of confidentiality, integrity, and authenticity.

Storing and accessing data in the cloud has its own challenges that compounded the classical issues of security. Today, an organization may choose to host its sensitive data in the cloud to harness the benefits of cloud computing and compete in the respective domain of business it relies on for day to day operations. However, when the data is sensitive its stewards need to implement the most rigorous security scheme that not only should provide them with the appropriate access level but makes sure that no data is compromised or leaked. The classical scenarios of security schemes may still be used. However, there is a limitation that comes with them. For instance, if the data need to only be accessed by the internal staff then a symmetric encryption scheme may be used and the key management is less of a concern but a key management control must be in place. On the other hand, if the data must be accessible to internal and external users, then an asymmetric scheme will be more preferable. In both scenarios, the cloud provider need to gain access to the key to perform usable functionalities against the encrypted data. This exposure of the key may not be acceptable due to the fact that the CP itself may be curious to know the nature of the sensitive data stored on its premises. To accommodate clients' security requirements, researchers are turning to the mathematical characteristics of fully homomorphic algorithms which enables search to be performed against encrypted data without the need of decrypting it.

In the rest of this paper we will examine different secure proposed solutions for accessing and transferring data in the cloud using different schemes that are based on the classical symmetric or asymmetric algorithms. Then, state the new solutions that are based on fully homomorphic schemes. These schemes are trying to solve the same problem which is securing data while enabling arbitrary calculation to be performed against it, except introducing asymptotically better performance in time and space. Finally, analyze these solutions in the paper conclusion based on the need of cloud computing in a multi-tenant environment and secure delegation computation.

Literature Review

Dent (2006) Cryptography is the branch of information security which covers the study of algorithms, protocols that secure data, and addresses several security properties mostly what's known as CIA. One of cryptography's goal is masking the plaintext to an unreadable format using a key to create a cipher text. Diffie and Hellman (1976) stated that classical cryptography systems are based on the NP-hardness of a mathematical problems, such as factoring two large primes or discrete logarithm. Authors also mentioned that these problems are said to be trapdoor functions because it is easy to compute the function one way, but extremely taxing to compute the reverse without some special information, known as the trapdoor. Diffie and Hellman (1976) classified cryptography schemes into two main categories: symmetric and asymmetric. Symmetric cryptography, uses one secret key for both encryption and decryption. Asymmetric cryptography "or public key cryptography" uses two different keys known as public and a private key, either of which can be used for encryption or decryption. The most widely used public key system is RSA, which relies on the factorization of two large prime numbers. In addition to the classical cryptosystems, scientists are researching homomorphic cryptography schemes to ensure privacy of data in