DATA INTEGRITY AND SECURITY IN CLOUD COMPUTING USING CRYPTOGRAPHY MECHANISM

Mrs. N.Manju#1, Mrs.V.Shanmugapriya*2

#1Research Scholar, Dept. of CS, PGP College of Arts & Science, Namakkal, Tamilnadu, India
*2Assistant Professor, Dept. of CS, PGP College of Arts & Science, Namakkal, Tamilnadu, India

Abstract—Modern technological advances have given rise to the popularity and success of cloud. This new paradigm is gaining an expanding interest, since it provides cost efficient architectures that support the transmission, storage, and intensive computing of data. However, these promising storage services bring many challenging design issues, considerably due to the loss of data control. These challenges, namely data confidentiality and data integrity, have significant influence on the security and performances of the cloud system. Some threat models assume that the cloud service provider cannot be trusted, and therefore security designers propose a high level security assurance, such as storing encrypted data in cloud servers. Others suppose that cloud providers can be trusted, and that potential threats come primarily from outside attackers and other malicious cloud users. Furthermore, a cloud user can never deny a potential server breakdown. Therefore, there are several challenges that need to be addressed with respect to security and privacy in a cloud context. This thesis aims at overcoming this trade-off, while considering two data security concerns. On one hand, we focus on data confidentiality preservation which becomes more complex with flexible data sharing among a dynamic group of users. It requires the secrecy of outsourced data and an efficient sharing of decrypting keys between different authorized users. For this purpose, we, first, proposed a new method relying on the use of ID-Based Cryptography (IBC), where each client acts as a Private Key Generator (PKG). That is, he generates his own public elements and derives his corresponding private key using a secret. IBC properties, this contribution is shown to support data privacy and confidentiality, and to be resistant to unauthorized access to data during the sharing process, while considering two realistic threat models, namely an honest but curious server and a malicious user adversary.

Key Words: cloud storage server, cloud computing, TPA.

I. INTRODUCTION

Many people are confused about what cloud computing is, especially as the term is overused. Roughly, it describes highly scalable resources provided as an external service via the Internet on a pay per use basis. Cloud computing can be defined as a specialized distributed computing model, which is dynamically configured and delivered on demand. This new massively scalable paradigm is different from traditional networks. It is highly abstract to deliver three levels of services.

Economically, the main attractiveness of cloud computing is that users only use what they need, and only pay for what they actually use. Resources are available to be accessed from the cloud at any time, and from any location through networks. There is no need to worry about how things are being maintained. The US National Institute of Standards and Technology (NIST) [PT09] provides a formal definition of the cloud computing as follows

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

In this sense, cloud users are raised to a level of abstraction that hides the details of hardware or software infrastructures, deployed for supporting intensive computation and data storage. From this definition, three main key points have to be considered. First, NIST outlines the development of technologies that support an omnipresent, universal and appropriate new business model. Second, it involves the importance of network access techniques to shared resources that assure a fluid interaction between the cloud providers and their clients. Third, this definition focuses on the associated pricing model of cloud which allows users to pay only for consumed resources.

To better understand the core concepts and technologies in the cloud, we extract from the NIST definition document [PT09] five attributes. These attributes describe a cloud based system as a general model providing metered on demand services to his clients. These characteristics are presented as follows:
PROBLEM STATEMENT AND OBJECTIVES

Cloud data storage services bring many challenging design issues, considerably due to the loss of physical control. These challenges have significant influence on the data security and performances of cloud systems. That is, cloud data are often subject to a large number of attack vectors, as depicted.

On one side, providing data confidentiality, in multi-tenant environments, becomes more challenging and conflicting. This is largely due to the fact that users outsource their data on remote servers, which are controlled and managed by possible untrusted Cloud Service Providers (CSPs). It is commonly agreed that data encryption at the client side is a good alternative to mitigate such concerns of data confidentiality. Thus, the client preserves the decrypting keys out of reach of the cloud provider. Nonetheless, this approach gives rise to several key management concerns, such as, storing and maintaining keys’ availability at the client side. In addition, the confidentiality preservation becomes more complicated with flexible data sharing among a group of users. First, it requires efficient sharing of decrypting keys between different authorized users. The challenge is to define a smooth group revocation which does not require updating the secret keys of the remaining users. So that, the complexity of key management is minimized. Second,
the access control policies should be flexible and distinguishable among users with different privileges to access data. That is, data may be shared by different users or groups, and users may belong to several groups.

On the other side, the data integrity is considered as a relevant concern, in cloud environments. That is, the responsibility of securely managing outsourced data is splitting across multiple storage capacities. Such distribution provides resilience against hardware. None the less, in order to reduce operating costs and save storage capacities, dishonest providers might intentionally slight these replication procedures, resulting in unrecoverable data errors or even data losses. There might be implementations of remote data checking at the three following levels:

- Between a client and a CSP
- Within a CSP
- Between two CSPs

These security concerns are even more important, as the European regulations will be more severe and inflexible, including further derogations to effectively protect personal data which are outsourced on remote servers.

- Objective A – improving data confidentiality in cloud storage environments while enhancing dynamic sharing between users. Indeed, the proposed security mechanisms should ensure both robustness and efficiency, namely the support of flexible access control, efficient user revocation and performances.
- Objective B – addressing the issue of provable data possession in cloud storage environments for data integrity verification support, following three substantial aspects: security level, public verifiability, and performance, and considering the limited storage and processing capacities of user devices.
- Objective C – implementing the proposed techniques using standards and widely deployed schemes, and validating their feasibility and impact on real hardware.
- Objective D – providing mathematical proofs of soundness and correctness of the proposed schemes

III. CRYPTOSYSTEMS

Attribute Based Cryptography

In 2005, Sahai and Waters introduced the concept of Attribute Based Cryptography (ABC) [SW05], as a new mean for encrypted access control. In ABC, ciphertexts are not necessarily encrypted to one particular user as in traditional public key cryptography. Instead both users’ private keys and ciphertexts are associated with a set of attributes or a policy over attributes. The user is able to decrypt a ciphertext if there is a match between his private key and the ciphertext.

This section gives a brief overview of ABC, as this cryptographic system is not addressed in this dissertation. However, it was interesting to introduce ABC, given its attractive features in cloud data storage environments. Interested readers may refer to [LCH13] for more details. In [SW05], Sahai and Waters presented a threshold Attribute Based Encryption (ABE) scheme. That is, ciphertexts are labeled with a set of attributes \( S \) and a user private key is associated with both a threshold parameter \( t \) and another set of attributes \( S_0 \). In order to decrypt enciphered data, at least \( t \) attributes must match between the ciphertext and the user private key. One of the primary original motivations for this work was to design an error-tolerant (Fuzzy) identity-based encryption scheme that could use biometric identities.

However, the disadvantage of KP-ABE is that the access policy is built onto one user private key. As such, the data owner cannot choose who can decrypt the data except choosing a set of attributes which can describe the outsourced data. In addition, the sender must trust that the key-issuer issues the appropriate keys to grant or deny access to the appropriate users.

Attribute Based Cryptography (ABC) is referred to as an innovative concept and one of the most attractive ways to manage and control file sharing in cloud, thanks to the computation properties on attributes. In fact, traditional access control architectures generally assume that remote servers storing the data are fully trusted by their clients. So that, they are often responsible for defining and enforcing access control policies. However, this statement does not usually hold in multi-tenant cloud data storage environments, especially due to the abstract nature of this business model. Consequently, cloud clients are still reluctant, while outsourcing their data file contents.

Homomorphic Cryptography

Homomorphic cryptosystems are cryptographic schemes whose encryption function are a homomorphism, and thus preserve group operations performed on ciphertexts. Homomorphic Encryption algorithms allow a third party to perform computations on ciphertexts, ensuring privacy preservation. In this section, we first introduce the concept of the homomorphic cryptography. Then, we give a review of some applications to homomorphic encryption schemes in cloud storage environments.

IV. PROPOSED APPROACH

41
In this first chapter, we present a general introduction to public key cryptography. We investigate the usage of attribute-based cryptography and homomorphic schemes in clouds. As a specific variant of attribute-based cryptography, we describe the ID-based cryptosystems which rely on the use of elliptic curve groups. ECC is a promising approach that significantly reduces the size of keys and encryption algorithms. Thus, it is well-suited for the security applications designed to resource-constrained devices. These cryptographic systems are referred to as interesting mechanisms, to mitigate cloud data security concerns, thanks to their attractive features. For instance, they provide much more flexible decryption schemes, and allow malleability on ciphertexts. Finally, we present some validation tools, namely the computational security and the provable security. In the next chapter, we leverage the usage of ID Based Cryptography in cloud storage environments. We propose an original ID-based client side encryption approach, where cloud clients are assigned the IBC–PKG function. So that, they can issue their own public elements and can keep confidential their resulting IBC secrets.

Fig1. Architecture of cloud data storage

V. CONCLUSION

In conclusion, we summarize how each of the research topics presented in the first chapter has been pursued, and the contributions which have resulted. Next, we reflect on how we can improve our contributions and provide new research directions. Throughout this thesis, our main objective was to propose efficient cryptographic mechanisms, in order to ensure data security in cloud data storage environments. We build upon the fact that cloud service providers are not totally trusted by their customers.

REFERENCES


