**INTRODUCTION**

Nowadays, the explosive growth of digital contents continues to raise the demand for new storage and network capacities, along with an increasing need for more cost effective use of storage and network bandwidth for data transfer. As such, the use of remote storage systems is gaining an expanding interest, namely the cloud storage based services, since it provides cost efficient architectures. These architectures support the transmission, storage in a multi-tenant environment, and intensive computation of outsourced data in a pay per use business model. For saving resources consumption in network bandwidth and storage capacities, many cloud services, namely Drop box, wale and Memo pal, apply client side

de-duplication. This concept avoids the storage of redundant data in cloud servers and reduces network bandwidth consumption associated to transmitting the same

contents several times. Despite these significant advantages in saving resources,

client data de-duplication brings many security issues, considerably due to the multi-owner data possession challenges. For instance, several attacks target either

bandwidth consumption or the confidentiality and the privacy of legitimate cloud users. For example, a user may check whether another user has already uploaded a file, by trying to outsource the same file to the cloud. Recently, to mitigate these concerns, many efforts have been proposed under different security models. These schemes are called Proof of Ownership systems (PoW). They allow the storage server check a user data ownership, based on a static and short value (e.g. hash value). These security protocols are designed to guarantee several requirements, namely lightweight of verification and computation efficiency.

Even though existing PoW schemes have addressed various security properties, we still need a careful consideration of potential attacks such as Data Leakage and poison attacks, that target privacy preservation and data confidentiality disclosure.

This paper introduces a new cryptographic method for secure Proof of Ownership (PoW), based on the joint use of convergent encryption and the Merkle-based

Tree, for improving data security in cloud storage systems, providing dynamic sharing between users and ensuring efficient data de-duplication. Our idea consists in using the Merkle-based Tree over encrypted data, in order to derive a unique identifier of outsourced data. On one hand, this identifier serves to check the availability of the same data in remote cloud servers. On the other hand, it is used to ensure efficient access control in dynamic sharing scenarios. The remainder of this work is organized as follows. The state of the art of existing schemes, introducing the general concept of PoW protocols and highlighting their limitations and their security challenges. Then, Section III introduces the system model. It presents our secure PoW scheme and gives a short security analysis. Finally, a performance evaluation is presented before concluding.