**INTRODUCTION**

Storage-as-a-service has emerged as a commercial alternative for local data storage due to its characteristics include less initial infrastructure setup, relief from maintenance overhead and universal access to the data irrespective of location and device. Though it provides several benefits like cost saving, accessibility, usability, syncing and sharing, it raises several security threats as data is under the control of the cloud service provider (CSP). CSP can discard the rarely accessed data to save space and earn more profit, or it can lie about the data loss and data corruption, as a result of software/ hardware failure to protect its reputation. Therefore, it is necessary to check the possession of data in the cloud storage.

Traditional cryptographic solutions for integrity checking of data, either need a local copy of the data (which the data users (DUs) do not have) or allow the DUs to downloads the entire data. Neither of these solutions seems practical as earlier one requires extra storage and later alternative increases the file transfer cost. To address this issue, several schemes including are proposed which employ block less verification to verify the integrity without downloading the entire data. One of the attractive features of these works is to allow the public verifier to verify. With public audit ability, DUs can recourse the auditing task to a third party auditor (TPA). It has expertise and capabilities to convince both the CSP and the DU. These schemes use provable data possession (PDP) technique, which gives probabilistic data possession guarantee by randomly verifying few blocks for ensuring possession of data in the un-trusted cloud storage.

Recently, several schemes have been proposed to allow TPA to check integrity of the data stored on the un trusted cloud. These schemes have their own pros and cons. prevent TPA to infer the data using the cloud server’s response while auditing. However, the schemes proposed in do not achieve privacy preserving requirement. Though data dynamics is an important feature to facilitate the data owners to insert, modify, and delete on a particular block of data, without

Changing the meta-data of other blocks, the techniques proposed in do not achieve data dynamics requirement. Meanwhile, the schemes like could not achieve batch auditing requirement which ensures that TPA should be capable enough to deal with the multiple numbers of simultaneous verification requests from different DUs. This property is to save computation and communication cost between CSP and TPA. Unfortunately, the schemes use pairing based cryptographic operations which are intensive computation and need more time.

In this work, we propose a secure and efficient privacy preserving provable data possession scheme (SEPDP) for cloud storage. It operates in three phases, namely, key generation, signature generation and auditing phase. Most attractive feature of SEPDP is that it does not use any intensive computation like pairing based operation. Further, we extend SEPDP to support multiple data owners, batch auditing, and dynamic data operations. A probabilistic analysis to detect the integrity of the blocks stored at CSP. We evaluated the performance of the proposed scheme and compared with some of the existing popular mechanisms.

We observe that the total time for verification carried out by TPA in the proposed scheme is less than that of the existing schemes. This signifies that SEPDP is efficient and suitable to implement the verification at the low powered devices. Remainder of this paper is organized as follows. dynamics requirements are explained in.