

**CHENNAI – PONDICHERRY**

**Three-server swapping for access confidentiality**

**Abstract:**

We propose an approach to protect confidentiality of data and accesses to them when data are stored and managed by external providers, and hence not under direct control of their owner. Our approach is based on the use of distributed data allocation among three independent servers and on a dynamic re-allocation of data at every access. Dynamic re-allocation is enforced by swapping data involved in an access across the servers in such a way that accessing a given node implies re-allocating it to a different server, then destroying the ability of servers to build knowledge by observing accesses. The use of three servers provides uncertainty, to the eyes of the servers, of the result of the swapping operation, even in presence of collusion among them.

**Existing System:**

The problem of ensuring data confidentiality in outsourcing and cloud scenarios has received considerable attention by the research and development communities in the last few years and several solutions have been proposed. A simple solution for guaranteeing data confidentiality consists in encrypting the data. Modern cryptographic algorithms offer high efficiency and strong protection of data content. Simply protecting data content with an encryption layer does not fully solve the confidentiality problem, as *access confidentiality*, namely the confidentiality of the specific accesses performed on the data remains at risk. There are several reasons for which access confidentiality may be demanded, among which the fact that breaches in access confidentiality may leak information on access profiles of users and, in the end, even on the data.

**Proposed System:**

We build on such an indexing structure and on the idea of dynamically changing, at every access, the physical location of data, and provide a new approach to access confidentiality based on a combination of *data distribution* and *swapping*. The idea of applying data distribution for confidentiality protection is in line with the evolution of the market, with an increasing number of providers offering computation and storage services, which represent an opportunity for providing better functionality and security. In particular, our approach relies on data distribution by allocating the data structure over three different servers, each of which will then see only a portion of the data blocks and will similarly have a limited visibility of the accesses to the data. Data swapping implies changing the physical location of accessed data by swapping them among the three involved servers. Swapping, in contrast to random shuffling, forces the requirement that whenever a block is accessed, the data retrieved from it (i.e., stored in the block before the access) *should not* be stored at the same block after the access. We illustrate in this paper how the use of three servers (for distributed data allocation) together with swapping (forcing data re-allocation across servers) provide nice protection guarantees, typically outperforming the use of a random shuffling assuming (as it is to be expected) no collusion among servers, and maintaining sufficient protection guarantees even in the presence of collusions among two, or even all three, of the involved servers.