

**CHENNAI – PONDICHERRY**

**CypherDB: A Novel Architecture for Outsourcing Secure Database Processing**

**Abstract:**

CypherDB addresses the problem of protecting the confidentiality of database stored externally in a cloud and enabling efficient computation over it to thwart any curious-but-honest cloud computing service provider. It works by encrypting the entire outsourced database and executing queries over the encrypted data using our novel CypherDB secure processor architecture. To optimize computational efficiency, our proposed processor architecture provides tightly-coupled datapaths that avoid information leakage during database access and query execution. Our simulation using a well-known database benchmark TPC-H over a commercial grade Database Management System (SQLite) demonstrates that our proposed architecture incurs an average of about 10% overhead when compared with the same set of operations without secure database processing.

**Existing System:**

A major deficiency in cloud security is that user data is stored in third-party servers in plaintext. Although it is assumed that the cloud service provider can be trusted by a contractual agreement, it does not necessarily imply that the server administrators are equally trustworthy. A recent security breach in Google shows that any server administrator with access to the confidential information can abuse it at ease. An even worse issue is that an honest-but-curious server administrator is capable of performing massive breach of privacy without being detected. One obvious solution to protect against such attack is by encrypting the outsourced database without revealing the encryption key to the administrator. However, it poses one daunting challenge: the computation on an encrypted data without the encryption key is at best very inefficient, or at worst impossible.

**Proposed System:**

To the best of our knowledge, CypherDB is the first to use processor architectural design to successfully protect remote operation on encrypted database against any honest-but-curious administrator.

We introduce a novel approach to encrypt the database that allows database operation to be performed efficiently and securely on CypherDB secure processor in a distributed database system.

We propose a run-time memory partitioning system to secure on-the-fly execution with a novel use of software-transparent cache line encryption and a per query random key.

We show that CypherDB, being able to support arbitrary database operations, requires only a minimal software changes and achieves well performance with only 10% performance overhead on average.