

**CHENNAI – PONDICHERRY**

**PRIVACY-PRESERVING DATA ENCRYPTION STRATEGY FOR BIG DATA**

**IN MOBILE CLOUD COMPUTING**

**Abstract:**

Privacy has become a considerable issue when the applications of big data are dramatically growing in cloud computing. The benefits of the implementation for these emerging technologies have improved or changed service models and improve application performances in various perspectives. However, the remarkably growing volume of data sizes has also resulted in many challenges in practice. The execution time of the data encryption is one of the serious issues during the data processing and transmissions. Many current applications abandon data encryptions in order to reach an adoptive performance level companioning with privacy concerns. In this paper, we concentrate on privacy and propose a novel data encryption approach, which is called Dynamic Data Encryption Strategy (D2ES). Our proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints. This approach is designed to maximize the privacy protection scope by using a selective encryption strategy within the required execution time requirements. The performance of D2ES has been evaluated in our experiments, which provides the proof of the privacy enhancement.