**CHAPTER-1**

**EFFICIENT AND PRIVACY-PRESERVING SIMILARITY RANGE QUERY OVER ENCRYPTED TIME SERIES DATA**

**ABSTRACT**

Similarity query over time series data plays a significant role in various applications, such as signal processing, speech recognition, and disease diagnosis. Meanwhile, driven by the reliable and flexible cloud services, encrypted time series data are often outsourced to the cloud, and as a result, the similarity query over encrypted time series data has recently attracted considerable attention. Nevertheless, existing solutions still have issues in supporting similarity queries over time series data with different lengths, query accuracy and query efficiency. To address these issues, in this paper, we propose a new efficient and privacy-preserving similarity range query scheme, where the time warp edit distance (TWED) is used as the similarity metric. Specifically, we first organize time series data into a kd-tree by leveraging TWED’s triangle inequality, and design an efficient similarity range query algorithm for the kd-tree. Second, based on a symmetric homomorphic encryption technique, we carefully devise a suite of privacy-preserving protocols to provide a security guarantee for kd-tree based similarity range queries. After that, by using the similarity range query algorithm and these protocols, we propose our privacy-preserving similarity range query scheme, in which we elaborate two strategies to make our scheme resist against the cloud inference attack. Finally, we analyze the security of our scheme and conduct extensive experiments to evaluate its performance, and the results indicate that our proposed scheme is indeed privacy-preserving and efficient.