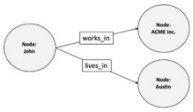
Encrypted Data Analysis Using Graph Database

[1]*Rapeti Tridev,*[2] *Shilpa Kapas,*[3] *Karunamoy Maji*
[1]*Department of Mathematics and Computing, IIT Kharagpur, India*
[2]*Ex-Intern, CET IIT Kharagpur, India*
[3]*Centre of Computational Data Science, IIT Kharagpur, India*
[2]*shilpakapas0@gmail.com*

Abstract

A cryptographic structural data paradigm designed to improve parallel and secure access to graph data. Our strategy focusses on breaking down complex social search queries into fundamental processes, carried out via adaptable protocols, guaranteeing rapid and scalable processing. To address the necessity of protecting privacy in graph query operations, we present a secure approach for inner product calculation. We subsequently enhance this strategy to meet various privacy standards under the known-background threat model. Our contribution involves creating an advanced framework that enhances efficient data retrieval while safeguarding the confidentiality of sensitive information. We aim to achieve a compromise between computational performance and privacy preservation by merging encryption techniques with parallel processing frameworks. This thesis examines the complexities of our suggested paradigm, clarifying its theoretical foundations and practical applications. We illustrate the effectiveness of our method in reducing privacy breaches while ensuring scalability and performance through thorough study and experimentation. This study makes a substantial contribution to the emerging domain of secure graph data processing, providing innovative insights and approaches for future research and development efforts.

(a) System Architecture



(b) Graph Database Model

The collaboration between in-memory and graph-based paradigms is crucial for enhancing efficiency across the data lifecycle. The rapid acquisition of information, along with the intricate depiction of relationships, enables analytics to be performed with maximum accuracy and efficiency. The integration of these two database models signifies a progressive technique, likely to enhance the realm of data management and processing substantially.