Abstract

Privacy preserving data mining has emerged due to large usage of data in organizations for extracting knowledge from data[1]. Big data uses centralized as well as distributed data and mines knowledge. Privacy preservation of data has become critical asset due to malicious users and society issues. It is very crucial nowadays to maintain balance between ensuring privacy and extracting knowledge. These areas is burning domain for researchers till now because no such research has been done that out performs all the techniques in privacy preserving data mining. Privacy preservation is classified into many categories like data modification, data distribution, data hiding and data encryption. For performance measuring, evaluation criteria like information loss, computational overhead, data utility etc are considered. Data modification techniques mainly focus on adding errors to data or results into output which degrades the accuracy of data mining algorithm. In case of critical analysis of data, crypto graphical approaches in privacy preserving data mining which has no loss of information but overhead of computation and communication have been adopted. PPDM includes homomorphic encryption, Shamir’s secret sharing scheme, oblivious transfer and many other cryptography techniques.
Challenges in this area include, higher computational and communication cost. At last, most advanced, functional encryption concept in privacy preservation have been included. Functional encryption provides higher level of security as well as privacy to data. It only allows learning output of function without revealing anything else.

References


Index Terms

Computer Science  Security
Keywords

FE, PPDM, STTP, TTP