69. ENHANCED SECURE MULTI PARTY PROTOCOL IN DISTRIBUTED DATABASES

J.JAYAPRABHA,Mrs.B.MOOHAMBIGAI,
M.E Student,Assistant Professor,
Department of CSE, Arunai Engineering College, Thiruvannamalai, India
jaicse18@gmail.com

Our protocol is based on fast distributed mining algorithm. The most important ingredients in our protocol are two novel secure multi party algorithm-one that computes the union of private subsets that each of the interacting player hold and another tests the inclusion of an element held by one player in a subset held by another.The sub-protocol used for the secure computation of the union of private subsets that are held by the different players.That is the most costly part of the protocol and its implementation relies upon cryptographic primitives such as commutative encryption, explicit transfer, and jumble functions.This part of the protocol inwhich the players may extract from their view of the protocol information on other databases, beyond that is implied by the final output and their own input.At the meantime such leakage of information renders the protocol not perfectly secure, then the perimeter of the excess information is explicitly bounded that such information leakage is safe, when acceptable from a practical point of view.The protocol offers enhanced privacy. In adding together it is simpler and is significantly more efficient in terms of communication rounds, communication and computational cost.

Keywords—Association rules, fast distributed mining algorithm, Advanced Encryption Standard.

ISBN 978-81-904760-6-5