ABSTRACT

Data related to individual wealth, financial status and health is sensitive and to ensure confidentiality of these data special mechanism is required. For betterment of research and development, requirement is right input from authorized users. Due to personal confidentiality concerns, it is very difficult to get individuals sensitive information even if it is for mutual benefits. To get the real time data from actual users is critical to achieve extraordinary quality research outcomes. In collaborative computation participants are unwilling to provide straight answers when the questions involve personal information. The service providers who collect's data need to establish substantial trust with the parties. The confidentiality and integrity guarantees of the proposed protocols can simplify this issue.

Privacy preservation is a big challenge for the data generated from various sources such as social networking sites, online transactions, weather forecast to name a few. The socialization of the internet and cloud computing generates pica bytes of unstructured data online with intrinsic values. The inflow of big data and the requirement to move this information throughout an organization has become a new target for hackers. The collaborative computation data is subject to confidentiality laws and should be protected.

People are more interested toward outsourcing work to a third party rather than maintaining their own resources, in this circumstance there is a requirement of insuring security from the service provider as it may lead to security breaches and party may not be interested in such service providers.

Secure multi-party computations deals with collection of challenges in which the requirement is the collaborative computation result. This computation needs input from multiple parties, but all the parties are concerned about their

individual input. The present research emphases on the domain of secure sum problem, in which all the participants are able to keep secret, the sensitive information about the individuals or the organization from other participants and computation authority (TTP). This individual sensitive information is not disclosed even after collaborative computation, apart from what is disclosed from final computation result.

This research proposes the protocols which increases confidentiality, security and anonymity during collaborative computation. Firstly, the thesis proposes a protocol for Secure Sum technique based on pseudorandom number called, "Joint Computation with Randomization and Anonymization" (*JCRA*), in this data confidentiality is preserved using pseudo-randomization. Secondly, an asymmetric encryption based protocol "Joint computation with asymmetric encryption" (*JCAE*) is proposed which could be applicable to generic secure multi-party computation problem; in this data confidentiality is maintained using encryptions. Thirdly, a distributed pseudo-randomization based technique "Distributed Randomized Secure Sum" (*DRSS*) is proposed in which confidentiality of data is improved by distributed pseudo-random number. Comparative analysis proves that the proposed protocol is more efficient when parameters like number of parties and confidentiality are concerned.

Intuitively, the proposed protocols are secure as: (i) Packetization ensures participant's that their sensitive data is secure during communication (ii) Anonymization ensures the anonymity, as it is hiding identity of individuals (iii) The confidentiality ensures that the other participant's cannot acquire any beneficial information about the parties' private inputs. For performance analyses following parameters are used; Number of party, Number of Anonymizers, Total number of packets per party. Validation and probabilistic analysis is carried out using simulation of the proposed protocol in the test lab setup.

The present research will be beneficial for those who are interested in collaborative computations, such as two person wish to find who is topper without revealing their actual marks to each other, Mobile service providers to get customer calling habit to attract customer or to find out total number of mobile users without sharing consumers details etc.

The methodology is structured to examine the techniques for cooperative computation. The implementation and testing of the presented protocols is done on VC++ for standalone implementation and in DotNet framework for network environment.

Finally, the research demonstrates and benchmark, the protocols. The comparative study is presented to demonstrate the performance analysis of protocols presented.