Consider a set of parties who do not have trust in each other, nor in the channel by which they communicate. Even then the parties wish to correctly compute some common function of their local inputs, while keeping their local data secure from others. This, in a nutshell, is the problem of secure multi-party computation (SMC). This problem is fundamentally in cryptography and in the study of distributed computations. It takes many different forms depending on the underlying network, on the function to be computed, and on the amount of distrust the parties have in each others and in the network.

In this tutorial, we present several aspects of secure multi-party computation like privacy of individuals, correctness of result and network traffic reductions. We first present the definition of this problem in various situations. Our definition is drawn from the previous idea and formulizations, and incorporate aspects that were previously overlooked. We also present several problems associated with SMC. Next we show the problem of hiding the data form trusted third party (TTP) which computes the result. We present the existing solutions of SMC along with the protocols developed by us. In our first solution, we introduced a randomly selected anonymizer between the parties and the TTP to hide the data. Apart from the randomly selection of anonymizer, the party will divide the data into number of packets and then send to different anonymizer so that the entire data will not reach to a single anonymizer and the privacy of individual will be maintained. After that, we present another problem, which enables the SMC to perform the correct computation of the result as well as the authentication of computational body. We have introduced multiple TTPs instead of a single one. If there is only one TTP then its behavior can be suspicious.

Using this multiple TTP concepts we have the option to choose a TTP from domain of TTPs for computation. In this method we divide the data in several packets and these packets are sent to multiple TTPs and a randomly selected master TTP will perform the computation after accumulating data from other TTPs. For the authentication of TTP, we have introduced the concepts of equivalence classes. With the help of this concept we remove the malicious TTP from the system for further computation.
Finally, present the problem of dealing with adversaries in SMC and minimizing their effects. We investigate the power of adversaries in several situations. We have also minimized the complexity of network traffic in entire process of SMC.

Author’s Biography

Dr. Durgesh Kumar Mishra received M. Tech. degree in Computer Science from DAVV, Indore in 1994 and Ph.D degree in Computer Engineering in 2008. Presently he has been working as Professor (CSE) and Dean (R&D) in Acropolis Institute of Technology and Research, Indore, MP, India. He has around 20 years of teaching experience and over 5 years of research experience. He has completed his research work with Dr. M. Chandwani, Director, IET-DAVV Indore, MP, India in Secure Multi-Party Computation. He has published more than 60 papers in refereed International/National Journals and Conferences including IEEE and ACM. He is a Senior Member of IEEE, Chairman of IEEE Computer Society, Bombay Chapter, India. Dr. Mishra has delivered his tutorials in IEEE International conferences in India and other countries. He is also a programme committee member of several International conferences. He visited and delivered his invited talk in Taiwan, Bangladesh, Singapore, USA, UK and several places in India in Secure Multi-Party Computation of Information Security. He is an author of one book and reviewer of three International Journals of Information Security. He is Chief Editor of the Journal of Technology and Engineering Sciences. He has been a consultant to industries and Government organizations like Sale Tax and the Labour Department of the Government of Madhya Pradesh, India.