Chapter 12
Secure Multiparty Computing Protocol:
A Secure Approach in Multiparty Computation

Zulfa Shaikh
Acropolis Institute of Technology and Research – Indore, India

Poonam Garg
IMT Ghaziabad, India

ABSTRACT
Secure Multiparty Computation (SMC) can be defined as n number of parties who do joint computation on their inputs $(x_1, x_2, \ldots, x_n)$ using some function $F$ and want output in the form of $y$. The increase in sensitive data on a network raises concern about the security and privacy of inputs. During joint computation, each party wants to preserve the privacy of their inputs. Therefore, there is a need to define an efficient protocol that maintains privacy, security, and correctness parameters of SMC. In this chapter, an approach towards secure computation is provided and analyzed with security graphs.

1. INTRODUCTION
Information is a resource of huge importance and economic value to individuals, public administration and private companies. This information is crucial, thus confidentiality and reliability play an important role in computation of actual results. Maintaining confidentiality and security from various sources/participants has become a challenge in today’s scenario. Security must be preserved in the face of adversarial behavior by some of the participants, or by an external party. Security perspective becomes a cumbersome issue in case of large number of participants. The most significant security issue is the protection of data. Some of the information security and data privacy challenges that hospitals face include lack of tough data protection laws, use of portable devices such as laptops by employees to store confidential information, rising data security costs due to increased employee background checks, training employees in maintaining data security, ensuring

DOI: 10.4018/978-1-4666-4209-6.ch012
Secure Multiparty Computing Protocol

compliance with security policies implemented in the hospitals, and problems through employee activity monitoring procedures. Benefits of confidentiality and information sharing leaves a huge yet unused potential for solving many problems of considerable economic value, for example secure auctions where no information besides the final price is revealed or information mining without revealing sensitive data. One of the technique found to handle three different important issues viz privacy, security and correctness is Secure Multiparty Computation (SMC). Formally SMC can be defined as n parties having their private inputs $x_1, x_2, x_3, \ldots, x_n$ respectively and these parties want to compute the value of the public function $y = f(x_1, x_2, \ldots, x_n)$ such that after the completion of computation no party has any information about the inputs of other parties apart from the information revealed by the computed result. The objective of SMC is to maintain security of the participating parties and to securely compute some function of their distributed and private inputs. The first such property that often comes to mind is that of privacy or confidentiality. The SMC model uses two computation paradigms; ideal model and real model. As per the ideal model all corrupt participants should learn no more from the protocol than what they would learn in ideal model. In ideal model any participant can know his input (obviously) and the result of evaluating function $f$. Another important property is that of correctness; this states that the output of the parties is really that which is defined by the function. All honest participants should receive the correct result of evaluating function $f$ because a trusted third party would compute $f$ correctly.

Most of the applications work on joint computation where large numbers of parties are involved. These parties send their data for computation to TTPs and the computing TTPs announces the result. The first major concern here is to maintain privacy of inputs provided by the parties. Security and correctness in the result of computation is the next parameter which has to be maintained in the protocol. This problem is SMC, where n parties send their private inputs $x_1, x_2, \ldots, x_n$ to TTPs for computation and TTPs announces the result in form of $y$. Privacy preserving data mining solutions is of great importance in the field of medical research. Consider the case that a number of different hospitals wish to jointly mine their patient data, for the purpose of medical research. Moreover, let us suppose that privacy policy and law prevent these hospitals from ever pooling their data or revealing it to each other due to the confidentiality of patient's record. In such a case, classical data mining solutions cannot be used, with the possible result being a slowing of the advancement of medical knowledge. Therefore, we provide privacy preserving data mining solutions that enable the hospitals to compute the desired data mining algorithm on the union of their databases, without ever pooling or revealing their data. In fact, the only information learned by the different healthcare centers is the output of the data mining algorithm.

The major concern with this computation is that, what if TTPs involved in computation are malicious? The results will be:

- Correctness in the output cannot be ensured.
- The malicious TTPs may affect security and privacy issues of SMC as well.

Formally SMC can be defined as a situation where there are n parties with private inputs $x_1, x_2, \ldots, x_n$ respectively and they want to compute value of public function $y = f(x_1, x_2, \ldots, x_n)$ such that after computation no party has any information about the inputs of any other party apart from the information revealed by the computed result. This computation can be performed in two ways by any organization. The first approach is, parties themselves performing the computation. The Use a trusted third party for computation.