CHAPTER 7

CONCLUSIONS AND FUTURE SCOPE

7.1 CONCLUSIONS

Confidentiality loss is the biggest loss in any business. Confidentiality leakage means revealing of information collection, usage, storage or private information to unauthorised users. Confidentiality loss could be personal or monetary. The asymmetric encryption techniques presented in the thesis gave new direction of work in multi-party computation environment. Expanding this work with more complex functionality in different simulation setup could be the next explorations.

Cloud computing is the future of computer science and it goes with outsourcing the work. The presented protocols could be implemented for cloud environment; it could be the direction for future work. The solution proposed in research work using asymmetric encryption technique could be extended for cloud computing but it is quite expensive.

To address real life problem such as disease control, city planning, secure auction and secure voting, it is required to integrate the individual personal data distributed across various resources. However these implementation needs confidentiality of individual data.

In the thesis, the SMC algorithm is evaluated for secure sum problem. In the future it could be designed to evaluate SMC algorithm for other problems like secure set intersection, set union etc.

In this research work, different approaches to solve secure sum problem, using secure multi-party computation technique has been presented as shown in *Table 7.1*, which assures confidentiality, security and anonymity of participating parties. With the increase in usage of cloud

computing and big data, outsourcing has gained importance. This research presented the solutions which guarantees confidentiality and security for all the participants but such a primitives are quite expensive and increases overhead if implemented in cloud environment. Thus any implementations which improve the efficiency at party and TTP level with fewer overhead in outsourced cloud computation would be of concern. Current, algorithms deals with SMC problems in which same result is disclosed to all the participants, and doesn't lead to any confidentiality loss. However there are few applications where the computation result could be different for each participant, that need to be communicated to the party only, disclosure of such result to everyone may lead to confidentiality loss. For example a laboratory has medical data to analyse the disease risk, but the party want to keep the result secret from third parties, because disclosure of such information to all others may lead to confidentiality loss and personal discrimination. In future it could be extended to solve such applications.

The best solution for the entire problems stated above is to acquaint a third party, who has the assurance and belief of all participants is called as trusted third party (TTP). The TTP will execute all the calculation after receiving the complete data from all the participants. The result is good enough until TTP is honest. As soon it losses trust of any participants the system will fail.

In the research work presented here, it was aimed to present design and development of techniques for privacy preservation during secure multi-party computations. Firstly, a protocol has been designed, a secure sum protocol using data hiding technique called as *JCRA* then, presented the parameters which affect the security and confidentiality of individual participants and evaluated the protocol to find computation complexity, confidentiality and security for secure sum problem.

Table 7.1: Outcome of Research

S. No.	Presented Algorithms	Result
1	*JCRA*	Confidentiality and security is achieved using pseudo random number '*r'*. This work fine for network as well as standalone environment. For data leakage in this protocol at least t_{pk} anonymizers and one party should combine.
2	*DRSS*	Confidentiality and security is improved. In previous algorithm if a party is compromised it can reveal '*r*' to curious anonymizer and data may be leaked to overcome that the multiple pseudo random number are used. One for each packet to increase confidentiality. It performs well in network and standalone mode.
3	*JCAE*	Confidentiality and security is significantly improved but throughput is dropped to 30%. As asymmetric key is used in this for security and confidentiality. Its working has been tested for standalone and network environment.

Secondly, the proposed protocol called as (*DRSS*) is presented to enhance the confidentiality by increasing the pseudo-randomization factor. It is compared with *JCRA* to analyze the performance in given set of conditions with different parameters.

Third protocol (*JCAE*) is based on asymmetric encryption techniques. This is a generic SMC protocol, which is used to increase the security level, here the data hiding technique is changed to asymmetric encryption and TTP will perform computation over the data after decryption. This protocol increases the computation complexity but reduces the communication and time complexity as compare to previous protocol (*DRSS*).

The computation complexity of the protocol is more. As confidentiality and complexity go hand-in-hand, so as the confidentiality increase then the complexity increase. The proposed protocols could be extended by adding extra TTP so that computational work can be divided among them for faster processing. According to analysis proposed protocol will perform better in case of semi-honest adversaries.

The protocols developed during this research, attains the basic objective of the research work confidentiality, security and anonymity. The outcome shows the results of joint malicious conduct are insignificant, if given set of constraints are followed.

7.2 LIMITATIONS

The proposed methodologies of SMC work satisfactorily when the difference between number of packets per party (t_{pk}) and number of anonymizers (m) is relatively less ($t_{pk} \leq m$) but it will perform better as number of anonymizers increases. The protocols work for unsigned integers for 32 bits only. Anonymizers are trusted and their job is only to route the packets. As protocol is providing confidentiality and security it will increase the cost and complexity. The protocols do not deal with different number of packets per party.

7.3 SCOPE FOR FUTURE WORK AND FINAL REMARKS

In the proposed work, different approaches to solve secure sum problem, using secure multi-party computation technique has been presented, which assures privacy and confidentiality. With the increase in usage of cloud computing, outsourcing has gained importance. This research presented the solutions which guarantees confidentiality and security for all the participants but such a primitives are quite expensive and increases

overhead if implemented in cloud environment. Thus any implementations which improve the efficiency at party and TTP with fewer overhead in outsourced cloud computation would be of concern.

Current, algorithms deals with SMC problems in which same result is disclosed to all the participants, and doesn't lead to any privacy loss. However there are few applications where the computation result could be different for each participant, that need to be communicated to the party only, disclosure of such result to everyone may lead to privacy loss. In future it could be extended to solve such applications. Currently, protocols are implemented for unsigned integers, but in future it could be extended for signed integers. In future research computation on Encrypted Data could be the scope (in order to decrease the computation complexity).

Finally, the stated objective is accomplished. In the initial stage of the research work the main challenge was to maintain confidentiality of the parties' private input from unauthorised access and securing parties from attacker and eavesdropper.

To maintain the confidentiality, the concept of pseudo-randomization and encryption was introduced. It prevents data from unauthorised access. To include anonymity, the anonymizers are used to hide the individual identity. During the research it has been observed that the broadcast of result may lead to inverse optimization, so the abstraction is maintain among the parties so that the information about total number of participants can be hidden. And as a result no participant can infer other participants' information from the result. In *JCAE* protocol asymmetric encryption is used to maintain high level of confidentiality. It reduces adversial attack.