7. Conclusion and Future Scope

Security issues in the area of cloud computing are active area of research and experimentation. Various issues are identified one of which is the security of user data and applications. Cloud services are available to achieve security with the varying techniques and methods. To address the challenge of selecting one of the cloud service based on the user requirements of security, an assessor tool is proposed.

Trust based evaluation is proposed in the form of trust model. It covers various aspects of security that are necessary to be checked at the time of cloud service selection. Trust value is the output of the trust model that measures the security strength. Strength in terms of various parameters is proposed for cloud services. Static and dynamic parameters are proposed and can be collectively used to evaluate security of the cloud services.

A test bed in terms of cloud environment is prepared and .net framework is used to evaluate the static trust value. Dynamic trust value can also be determined and solutions are proposed to evaluate the parameters. Cloud services are studied and analyzed to evaluate the trust value. The effectiveness of the trust model is observed by the trust value calculated by using the parameters. Trust model is also validated against the solution measures for the security challenges given by the CSA service. Almost all aspects of security can be measured from it.

Trust model can be effectively used by the user to select a particular service. It can also be used by providers as a benchmark to find out the shortcomings and improvement areas of a cloud service or application. Trust model can be integrated with the cloud services and their descriptions as a cloud service manager. Cloud service manager stores trust value repository of registered cloud providers and their services. The trust value measures can be used to select a service globally by the users.

7.1 Major Contributions

The major contributions from this research is analyzing cloud computing security issues and proposing trust evaluation scheme for security of a cloud computing application or service. The contributions are listed below.
Measuring the security strength in terms of trust is done for the first time in the area of cloud computing.

A trust model formulated that evaluates the security strength is proposed.

Static trust calculation by using static parameters is the outcome of the trust model.

Making the model dynamic by considering dynamic aspects of security is also proposed.

Adequacy and the accuracy of the model are evaluated.

Trust model acts as a Security Strength Evaluator and Benchmark for a Cloud Computing Service.

7.2 Future Scope

Cloud Computing security challenges are part of ongoing research. Various open issues are identified as future scope.

- **Data Classification based on Security**: A cloud computing data center can store data from various users. To provide the level of security based on the importance of data, classification of data can be done. This classification scheme should consider various aspects like access frequency, update frequency and access by various entities etc. based on the type of data. Once the data is classified and tagged, then level of security associated with this specific tagged data element can be applied. Level of security includes confidentiality, encryption, integrity and storage etc. that are selected based on the type of data.

- **Identity management system**: Cloud computing users are identified and used their identities for accessing the services. A secure trust based identity management scheme is essentially a need by all cloud service provider and users. Various issues of identity management system are identified. Solution to secure id-generation and distribution, storage and life cycle management is a demand for trust based identity management system.

- **Secure trust based Solution for cloud computing Service**: A secure environment for execution of the cloud computing services along with overall security considerations is a challenge. A secure and trusted solution is the requirement that needs to be focused and addressed by the cloud computing infrastructure.
• **Optimization of resource Utilization:** Security considerations and provisions for virtualization along with the optimum use of the cloud infrastructure also needs to be focused and addressed.