CHAPTER 7

CONCLUSION AND FUTURE SCOPE

Implementing robust security and privacy strategies in distributed systems is a challenging issue. This research work makes a step forward in solving this issue by proposing a generic framework for multi-factor authentication to protect services and resources for unauthorized use. The authentication would be based on trust-based systems. Proposed framework would not only demonstrate how to obtain secure multi-factor authentication, but also would be addressing several prominent issues bio-inspired computing applications. To deal with different uncertainties in the proposed model, fuzzy logic has been used. The rule base systems are implemented using fuzzy knowledge base approach.

The main characteristics of the proposed approaches are

- Identification of basic security parameters.
- Definition and implementation of security parameters and their inter-relationships.
- Identification of bio-inspired security issues
- Integration of trust based model.
Trust values have been used to perform authentication and access control, ensuring a secure grid environment. Fuzzy logic concept is utilized for evaluating the trust. In future, authors would be working for decreasing the computations required for generating and updating trust values. Also reputation parameter can be added to ensure secure communication.

Having dealt with high risk security attacks in distributed systems trust based distributed systems are extremely applicable. Integration of cryptographic methods is an excellent effort towards the development of extremely secure distributed systems. The DNA based cryptography method is integrated with a rule based post processing method dealing with security attacks in the distributed systems.

I would like to conclude the present thesis with proposal that the work in the thesis can be extended by applying robust bio-inspired mechanisms and computational intelligence approaches.