ABSTRACT

In day-to-day life, the technical challenges that face in pervasive computing environment are going in a rapid rate. In order to provide security, these challenges also raise questions about the issues like privacy and trust. So, to provide a secure reliable communication between the user and system environment we develop an enhanced privacy model with dynamic trust engine in a pervasive environment. In this thesis work, to address the security issues, a new security model is developed which will protect the attackers present in the environment and also a privacy model is developed which will be used to preserve the privacy of the user or data being maintained in a network.

In Security model, mainly we focus on DDOS attacks and the mechanisms which will address the problems of the attacks that occur in pervasive environment at different layers like network layer, transport layer and application layer. Thus a model for checking of reliability with single path and multipath routing technique is developed. Also proposed solution is carried out by a network simulator for mobile ad-hoc networks in pervasive environment.
Data globalization is the technique to substitute the values of sensible information with more common values. Data virtualization means users can access data without any concern for where it resides, what the technical interface is, how has it been implemented which platform it uses and how much of it is available. The virtualized data in a table which may be thought of as an added field or diminished field in the original master table so that each tuple representing a unique data as in the original master table. The mapping between original and replicated data is done by careful data enriches. Data embellishment is elaborating or hiding the values of that information as many times as possible.

In order to evaluate privacy in the quantitative method, the privacy handled by many covered entities, the amount of acceptable uncertainty in each and every exchange is considered. The privacy can be determined by the product of final trust for an entity and anticipated risk, where final trust can be evaluated by maximum trust considering all roles and responsibilities and relationships played by the entities and risk can be evaluated by minimum risk from the entity. So, the privacy information flow includes the processes from Authentication process, Authorization process, and Trust evaluation process, Compliance checking process, Risk calculation, Privacy calculation process and Decision making process. This quantitative approach can be applied in small size of infrastructural facilities available in the environments.
As a pervasive computing environment can come in different formats such as static networks (e.g. sensor network), mobile networks (e.g. MANET), and wireless networks (e.g. Pure and Managed), the requirements given by the security and privacy issues take a major role and these can be solved by above said mechanisms for a maximum of satisfaction level in the network.