The Peer-to-Peer (P2P) is an emerging model and is being widely adopted in today’s internet computing. A P2P network is composed of an unbounded set of peers, where different users and organizations share their computing resources such as processing power, memory storage, disk space etc. in a completely distributed, scalable and fault tolerant manner. The P2P traffic contributes the largest portion of the internet traffic which is unnecessary and lead to delay.

The simplicity of blind flooding makes it very popular in practice. This mechanism relays a query message to all its logical neighbors except the incoming peer and incurs more traffic overhead. Current P2P systems are facing more challenges from security problems. The methods and techniques developed for query processing, traffic incurred by them is mainly focused on traffic issues, but not on the security problems.

This research is an attempt, guided by the motivation of reducing query response time, traffic cost incurred by the P2P network and security problems during transmission of data from one peer to another peer. This research has been performed to reduce the query response time and traffic overheads in P2P environment and thereby securing information by selecting an efficient query-forwarding paths and logical neighbors. As a result, it reduces the query response time, traffic cost and provides the more number of satisfactory
transactions which increases the overall system efficiency and Quality of Service (QoS).

This thesis aims at presenting a robust system and solutions for reducing query response time, traffic cost and providing healthier environment by avoiding unnecessary messages, message duplications and malicious transactions. After a review of the previous work is this area, it is proposed to design an unstructured RQR (Reduction on Query Response Time) where each and every peer can perform both probing and computing. Also, it does not have bootstrapping node to monitor the query message transactions. Along with the traffic issue, the proposed design is more concerned about security problems which are addressed by implementing Optimal Reputation model (ORM) technique.

The design of RQR - This system is an efficient method to select query forwarding paths and logical neighbors. In RQR design, all peers who are connected in the network are in ready state to probe or compute the queries. The optimal path algorithm finds all the possible paths existing from source to destination peer along with the optimum path through which the query can be forwarded. The queries are forwarded through the optimal path and the time delay between peers is recorded in the form of adjacency matrix. Initially time stamp is assigned along with system time for peers. If any peer is not arrived response within the time quantum given to them, then the queries are resent and the waiting time is calculated along with the processing time.
Computation of Query Response Time (QRT) - Response time of a query is equal to the time period from when the query is issued until when the source peer receives a result from the first responder. The same process is continued for “n” number of queries. The query response time is recorded for the proposed RQR design with different time interval to prove the consistent system performance.

The Traffic Overhead in RQR – The traffic overheads incurred to establish the RQR design throughout the entire snapshot and performance evaluation of network is about 70 percentage lesser than the previous system which is SBO (Scalable Bipartite Overlay network) model, Since the RQR design does not have central control to maintain the information and it is designed as simple as possible.

The Optimal Reputation Model (ORM) – This technique is used to secure messages during transferring messages from one peer to another. The provider is accountable for all its past transactions. Every peer maintains its past transactions. Every peer has track of transactions from source peer to destination peer and store it in data base called query message history table (MHT). This MHT has the records of all transactions. Based on the transaction value assigned to them, the transactions are categorized as satisfied transactions (ST) or unsatisfied transactions (UST). Finally, the trustworthy peer is identified based on the number of satisfactory transactions and through which query message transactions are performed.
The performance benefit of RQR is consistent with different time intervals and with different amount of queries. RQR achieves about 50% of reduction in query response time. Our experimental results show that RQR comparatively outperforms existing approach. In ORM, the reputation of the provider is considered and the reputation of the requester is ignored. Further, this system can be extended to encapsulate the reputations of both the provider and the requester.

The experimental result shows that the average number of satisfactory transactions of optimal reputation model is about 50 percent more when compared to RSA blinding cryptographic algorithm and reputation model. The number of messages destroyed in RSA blinding is higher, so its overall performance in dynamic environments is not as good as Optimal Reputation model. Also, the performance of the ORM is compared with other reputation-based models namely, P2P reputation model and Pseudo trust. The result is about 50 and 60 percent respectively and is lesser than ORM.

This research has been performed to reduce the query response time and to secure information in P2P environment by selecting efficient query forwarding paths and logical neighbors. As a result, it reduces the query response time, traffic cost and provides more number of secured transactions which increases the overall system performance.