ACKNOWLEDGEMENT

It is my pleasant duty to thank a large number of people for the various forms of help, encouragement and support that they have provided during the time I have been working on this thesis. I would like to express my deep and sincere gratitude to my PhD Supervisor Dr. Vidhyacharan Bhaskar, Professor, Department of Electronics and Communication Engineering, for his invaluable guidance with innovative ideas, constant support, immense knowledge, motivation and enthusiasm. His understanding, encouraging and personal guidance have provided a good basis for the present thesis. I consider myself extremely fortunate to have had a chance to work under his supervision.

I am equally thankful to Dr. Gaurav Bajpai, Senior Lecturer, Department of Computer Engineering and Information Technology, Faculty of Engineering, Kigali Institute of Science and Technology, Rwanda for being my research coordinator and for his ideas and suggestions that helped me a lot in finishing my research work in time. It has been a very enjoyable experience to work under him.

I convey special acknowledgement to Dr. T. R. Pachamuthu, Chancellor and Prof. P. Sathyanarayanan, President of SRM University. I extend my sincere thanks to Dr. M. Ponnaikko, Vice Chancellor, for allowing me to do my research in this prestigious institution. I would also acknowledge and give special thanks to
Dr. C. Muthamizhchelvan, Director (E&T), Dr. S. Ponnusamy, Controller of Examinations, and Dr. Kasmir Raja, Dean (Research) for their support.

I gratefully thank Dr. S. Malarvizhi, Professor & Head, Department of Electronics and Communication Engineering, for her advice and constant encouragement.

I warmly thank my Doctoral Committee members, Dr. A. Gopal, Assistant Director, CEERI, Chennai and Dr. S. Jayashree, Professor & Head, Department of Electronics and Communications Engineering, Adhiparasakthi Engineering College for their valuable advice and extensive discussions around my work.

I wish to thank my colleagues Dr. Jaya Shukla, Mr. Sam M. Job and Dr. Godwin Asemota for their valuable discussions and constant support during my research work.

I express my sincere thanks to all the teaching and non-teaching staff of Department of ECE, SRM University, my family and friends who helped me directly and indirectly to carry out this work. Finally, I extend a special thanks to my daughter R. Nikitha for her care, affection, and patience during the research work.

P. M. RUBESH ANAND
ABSTRACT

Peer-to-Peer (P2P) networks and applications are the recent attractions among the users in the internet world. The benefits like high scalability, anonymity, self-organization, low operating cost, and low barrier of entry has made P2P content sharing network as one of the highest internet traffic generators. The peers’ success rate in receiving their intended content through P2P content sharing network is always low due to problems like free-riding, content pollution, content poisoning, content availability, DoS attacks, and flash crowd. These problems lead to consequences like wastage of peers’ time, bandwidth, and other resources. The aim of this research work is to solve all the notified problems of P2P content sharing network in a single unified model that combines trust management and security.

In public P2P networks, efficient utilization of bandwidth during content sharing is the primary concern. The proposed unified model helps in saving bandwidth from unnecessary wastage through controlled scalability. Controlled scalability is considered with appropriate algorithms for optimization of bandwidth utilization by peers in the P2P network. A strong mathematical model is developed in support of this for theoretical analysis and its solutions help in designing the practical P2P content sharing network. High scalability is an important property of public P2P networks and the proposed model overrides it by implementing restriction to it in the initial stages of the overlay network expansion. Decision
support for network restriction and expansion at different stages of the model is aided by the necessary algorithms. This restriction has efficiently solved problems like bandwidth wastage, content pollution, and flash crowd.

Mathematical modeling and analysis of the proposed unified trust management model is tested for verification in the real-world environment through appropriate simulation parameters. PeerSim is used in event-driven mode as a P2P network simulator for simulating the proposed model. Performance measures, such as scalability, content availability, flash crowd, and prevention of polluted or infected content distribution are compared with BitTorrent simulation in both homogeneous and heterogeneous environments. From the simulation results, it is observed that the proposed trust management model efficiently resolves trust and security issues in P2P content sharing networks. BitTorrent is taken as a benchmark for performance comparison due to its success and acceptance among the internet community. Moreover, such comparison helps in deploying the proposed trust management model in BitTorrent-like P2P networks for improving the existing systems’ performance.

Private P2P networks have additional security mechanisms like authentication schemes and random number generators in secured content sharing compared to that of public P2P networks. Though the existence of private P2P overlay networks is invisible to the public domain, they are often vulnerable to information theft and attacks. The mathematical modeling and analysis of private
P2P networks use the same idea as that of public P2P networks, except authentication and cryptographic mechanisms.

Independent feasibility studies are performed on 3D handwritten signature biometrics and random numbers generated through novel methods for its usage in private P2P networks. In the authentication mechanism, a prototype system for 3D signature acquisition and verification with pattern recognition techniques is developed and tested. The results indicate that the depth information of handwritten signature acts as a distinct hidden factor and shows a positive sign for consideration as a unique biometric identifier.

In random number generation for cryptographic applications, two novel methods are proposed for generation of uniformly distributed random numbers. In the first method, quaternion Julia fractal images are generated and demonstrated with symmetric encryption and decryption in visual cryptography. The second method of generation of random numbers is by utilizing astronomical data at different times and locations. Both methods show better randomness compared to the existing random number generators. The proposed authentication and random number generation mechanisms demonstrate a new type of enhanced security for private P2P networks.