Preface

Computer architecture and large-scale data processing mechanisms have refined day by day. In its evolution, we can note few paradigm shifts that were responsible to take the evolution to next level. However, the continuous improvements in computing infrastructure, in the recent years, the users have produced a flood of data, demanding improvement in large-scale data processing technologies.

With such progress, we find the necessity of new approaches to harness the potential of cloud in data storage and processing. Large-scale data processing systems are being developed for managing the vast data produced and processed. Though we have seen many big companies already developing and using such large data processing systems, we find an ultimate goal of having a system that anyone can deploy quickly on Cloud infrastructure, such infrastructure still not satisfied. Cloud service provider can ensure the user's data security using the concept of firewalls, virtual private networks, and by implementing other security policies within its own periphery or perimeter. Since, the resource pooling concept of the cloud requires to exchange information and data with other cloud owners, and also business critical or other relevant data of the client is available not only to the cloud but also to a third party cloud. Security, therefore, is a major challenge in any cloud computing infrastructure, because it is essential to ensure that only authorized access is permitted, and secure behaviour is expected.

Our focus in this work is to explore the cloud computing issues and challenges with the aspect of security, especially identity and access control management for cloud computing. Managing identities and access control for enterprise applications remain one of the greatest challenges for ÍT industries.

Research work presented in this thesis has three parts. In the first part, we have given an integrated model for authentication in cloud computing scenario based on pretty good privacy and Kerberos protocol for network security. There are several methods and mechanisms as well as ideas are proposed and presented to achieve security in the cloud.

We have proposed a novel method to achieve fine-grained security with combined approach of PGP and Kerberos in cloud computing. The proposed method provides authentication, confidentiality, integrity, privacy and non-repudiation features to Cloud Service Providers and Cloud users. The second part of our research work presents an authentication approach based on mobile One Time Password (OTP) verification system. Authentication is the very prime concern to protect the sensitive information. Failure in protection of such information can lead to losing of clients in several fields i.e. banking sector, national security, and cloud infrastructure etc. Today, SMS-based OTPs are commonly used for authentication and authorization for many applications. One-time passcodes are one of the fastest and easiest ways to provide strong authentication to any user anywhere. One Time Passwords (OTPs) are sent to the users via email or SMS text message, providing a second authentication factor when logging into any cloud infrastructure.

Finally, we have given a strong authentication mechanism based on multifactor such as biometrics, tokens, OTP, etc. The proposed method will be helpful in managing access control efficiently. As a part of the security within cloud computing, various services and resources need protection from unauthorized users. Authentication is a crucial technology for information security. Remote authentication is the commonly used method to determine the identity of the remote client. In this chapter, we proposed a systematic method for authenticating clients, namely by using a password, biometrics and out of band based mechanism that is suitable for access control. The proposed system involves user’s Id/ password, biometrics characteristics and a mobile phone as a software token for One Time Password generation.