Chapter 1

INTRODUCTION

1.1. Background

The continuous improvement in computing infrastructure, in the last two decades, has produced a flood of data demanding improvement in large-scale data processing technologies. Cloud computing has emerged with major advantages in data storage technology and sharing of resources. In cloud computing, one you can retrieve folders or files, facts, sequencers and third-party facilities from a web browser over the web which is hosted by an external vendor. We have to compensate for the possessions and computer service station that we use. We are witnessing a continuous growth of computational technologies and consequent data generation during the past few decades. With the development of web technologies, users now generate and consume large amounts of data on the Inter net. Cloud computing has provided a pattern change in the distribution of resources across the network, reducing the administrative costs associated with the IT infrastructure. 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 big data. Many issues and challenges exist in cloud computing. Some problems are safety, identity managing, source managing, energy and energy managing, source obtainability and source heterogeneity. Among all these problems, security is vital.

Since many IT companies develop and use secured system, we need such a secured system that anyone can deploy easily on Cloud infrastructure. Firstly, we have to ensure security from insiders, because it is easy for an initiator to access credentials. Secondly, there must be some mechanism for authenticating the user i.e. the customer, since data across cloud under the supervision of an external cloud service provider (CSP).

1.2. Motivation For the Work

- In the cloud, there is no user control over the data; on the other hand, the cloud provider receives an unjustified ability to excel in client data, including access control policies in the data.

- The cloud service provider can be self-centred, unreliable, and probably malevolent in relation to client data (internal threat).
- There is a lack of security over customer data on "Trusted Computing (TC)" technologies, because data are controlled by a third party and does not give data owners complete control over data protection your data.

Due to the above problems, data owners are antipathetic to handover their sensitive data to the cloud because of privacy issues and data integrity. Therefore, the need to provide more data security in the cloud environment leads to the study of methods for protecting client data in the cloud, including from the cloud providers themselves.

1.3. Objective of the Thesis

The primary goal of this thesis is to study the security related obstacles in acceptance of cloud computing and based on that investigation we focus our objective to propose approaches to enhance the security of cloud user as well as providers data and personnel information privacy. Design and development of efficient frameworks for cloud computing by using suitable authentication factors and methods to improve the security of cloud computing are the ultimate concern.

1.4. Contributions

The main contributions of this thesis are as follows:

- This research investigated and presented the brief analysis of various challenges and issues in the security domain of cloud computing.

- Proposed a new Pretty Good Privacy (PGP) and Kerberos-based approach for authentication method in cloud computing that offers validation, secrecy, reliability, and confidentiality purposes for cloud facility suppliers and cloud computing consumers.

- Proposed an approach for authentication method using mobile verification system. In this approach, we aim at both user and cloud service provider to authenticate their identity when they adopt the cloud computing services and applications.
- Proposed an efficient hybrid framework for authentication using multifactor authentication approaches such as biometric, OTP and user id and password.

The brief study (survey) has given related to existing security and privacy barrier in cloud computing.

1.5. Organization of the Thesis

The organization of this thesis is as follows:

Chapter 1 arrange for the introduction, motivation and problem description for the present work including thesis scope/objectives, and contributions. Finally, the chapter concludes with the organization that describes the coverage of chapter in the thesis.

Chapter 2 presents the theoretical background linked to cloud computing. The section gives brief cloud computing issues and challenges. Main emphasis is given on security.

In **Chapter 3**, we focused on authentication methods in cloud computing and proposed a suitable authentication framework to improve the security and secrecy in cloud computing. The planned outline utilizes the features of Pretty Good Privacy and Kerberos protocol to enhance the secrecy and safety of the users that adopt the cloud computing.

In **Chapter 4**, we present an approach for authentication method using mobile verification system. In this approach, our aim is related to both user as well as cloud services provider to authenticate their identity when they adopt the cloud computing services and applications.

In **Chapter 5,** we present an authentication mechanism that uses several authentication factors to authenticate cloud service providers and their users to protect their private data and information.

In **Chapter 6,** we summarize main findings of the thesis and give future direction of the research in the area.