1. Introduction

Cloud computing has become a part of the competitive market today. Many organizations make use of cloud services. Although cloud computing services is growing and gaining popularity, the fear about the usage of cloud services is still an open issue. Various issues deterring adoption are identified in the literature; one of the major ones is security. Security risks in the area of cloud computing has attracted attention since its beginning. New protocols and tools are always in demand to enhance the security strength of a cloud computing service or service provider.

Various cloud computing service providers are available with their services in the cloud environment. These services come along with various specifications, features and methods of achieving security. Some services focus on secure access to a service and data by encryption, and some are focusing on secure network itself. Techniques adopted by various providers to achieve security are of varying nature. A cloud user may seek a service based on his requirement and level of security provided by a service. To analyze a particular service based on its various security properties is a challenge. The major challenge is to trust a cloud service or service provider in terms of security. One can attempt to model such ‘confidence’ in a cloud service, as a kind of trust value. This thesis explores the possibility of building such a framework for trust computation, and its various aspects.

The thesis presents a trust based evaluation that a cloud user can use to determine trust of a cloud computing service. A trust model is formulated that can measure security of a cloud application or service. Trust model measures the security strength and gives a trust value. A trust value consists of various parameters that are necessary dimensions along which security can be measured. These parameters depend on sub parameters and functions that are measurable units. The overall trust value that can be calculated in the form of various parameters is termed as static trust.

Over a period of time service usage and user experience gives sources for the dynamic behavior of the trust. Dynamic parameters are formulated based on these sources and makes the model dynamic. Static and dynamic parameters both can be used and evaluated to determine security strength of a cloud computing application or service. Trust model can be used by cloud user to
evaluate the cloud service security, and a cloud provider can use it to find out the shortcomings and improvement areas. Thus trust model acts as a benchmark or a ranking service to evaluate security in a cloud computing environment.

1.1 Overview of Cloud Computing

Cloud Computing is a type of computing infrastructure that consists of a collection of interconnected computing nodes, servers, and other hardware as well as software services and applications that are dynamically provisioned among competing users. It focuses on delivering reliable, secure, fault-tolerant, sustainable, and scalable services, platforms and infrastructures to the end-users. These systems have goals of providing virtually unlimited computing and storage, and hiding the complexity of large-scale distributed computing from users. Services are delivered over the Internet or private networks, or combination of these. The cloud services are accessed over these networks based on their availability, performance, capability, and Quality of Service (QoS) requirements.

Depending on the type of service provided, there are three types of cloud services also termed as delivery models; Infrastructure as a service, (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

- IaaS deals with providing computing facility, storage or any other hardware resource. Amazon is one of the cloud providers offering IaaS. Examples of these services are EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service).
- PaaS provides platforms in terms of operating system and any other system software that can be used to build custom applications by the users. User can configure and develop their application on the specific platform. Microsoft Azure is an example of PaaS.
- SaaS deals with using any application or service via cloud. Google calendar is one of the examples that provide collaboration on various applications, like event management, project management etc. via internet. Salesforce is also a common and popular example of CRM SaaS Application.
1.2 Features and Benefits

Cloud computing started its base in the mid of 2007 and is growing rapidly so far. It has various features that make users to switch to the cloud computing environment. Some of these features are discussed below;

1. **Elasticity and Scalability:** The cloud resources can be provisioned or de-provisioned as per the increase or decrease in the user demand. The computing power, memory and other facility can be scaled up or down as per the user requirement.

2. **Ease of use:** There is no need to own and maintain expensive hardware, software and other resources by the cloud user. The cloud services are directly accessed using a web browser. No extra resources are needed to run and execute cloud services. A simple desktop with normal internet connectivity is sufficient.

3. **Device and Location Independent:** Since the cloud services can be accessed through web browser, it can be accessed geographically from anywhere and from any device that supports web interface. A cloud service can be accessed like any web service.

4. **Provision for custom application development using PaaS:** Software development using PaaS is easier compared to in-house application development, which requires hardware and software support as well as necessary development tools to be owned, installed and managed. In cloud computing environment, development tools and software are available in the form of service, which makes development easy and faster.

5. **Reduced cost:** For making an entry in to a business, cost required for infrastructure is reduced by moving to the cloud. As computing power, storage and other resources are used from cloud; cost to purchase as well as manage them is greatly affected. It is advantageous for the organizations if the resources are needed by them only for small duration and also when the need arises in course of time.

6. **Multi-Tenancy:** A single data server, computing and other resources are shared among multiple users by using virtualization and isolation. This feature termed as Multi-tenancy, allows efficient utilization of resources.
7. **Reliability**: Multiple channels are available for computing power, storage etc. for providing more reliable services to the users. Also the data may be stored at multiple locations by provider. This redundancy in terms of data storage and other resource enables provision for disaster recovery and achieves better reliability and availability of data as well as services compared to what one can manage when all these are to be provided at one’s own premises.

The above features of cloud computing makes it suitable for various organizations and users. But along with benefits and features, cloud computing also suffers from various issues acting as obstacles for its adoption. A few of them are discussed in the next section.

### 1.3 Obstacles for Adoption

Along with advantages for using cloud computing applications and service, there are some obstacles that act as a barrier in its growth. They include:

1. **Lock-in**: It is the problem of portability and Inter-operability. Lock-in issue could be for data and vendor.

   **Data Lock-in**: Data stored at one cloud site cannot be easily taken back, if a user wishes to change a cloud provider. It may be due to lack of standardized API. This results in a problem of data lock-in.

   **Vendor Lock-in**: A cloud provider gives services in terms of APIs. API made for one provider of cloud may not be useful for another provider’s cloud. If a change of provider is required then APIs also has to be changed, leading to at least partial re-development of the application. This issue is termed as vendor lock-in.

2. **Service Availability**: For a cloud user, service should be available at all time. Whenever a user requests for a cloud service, provider and user has to sign SLA (Service Level Agreement). This defines the terms and conditions and specifications for cloud service. It also includes percentage of time service is available. A cloud user expects a high available service with no or minimal downtime. A cloud provider and its corresponding service, is selected based on service availability and business needs.

3. **Bottleneck**: Data transfer bottleneck and service disruption are some of the issues caused due to bandwidth limitation.
4. Data privacy: For various organizations, concerns about security, privacy, compliance and control over their data are obstacles in moving towards adopting a cloud model. Specific concerns include:

**Loss of governance:** A cloud provider site is located in one country and the cloud user using the service from another country. User data which is stored from one country is owned and is under the control of cloud provider country. The data, therefore, may be outside the organization’s direct control, despite it being the owner and creator of the data. Its misuse may have a significant impact on privacy, security and intellectual property claims.

**Regulatory compliance:** This property states that though data may reside in the cloud, the obligation for regulatory compliance may still falls with the organization that owns the data and hence is implicitly responsible to any issues arising out of the cloud provider’s misuse.

**Lack of transparency:** Cloud vendors do not always disclose the details of how their services work, which third-party partners they use, and exactly where the data is located. The information about the user data, security measures etc. are generally not known to user.

For global businesses with offices and users in different countries, the issues are even more complex, as legal requirements and provisions vary between countries.

Such obstacles as discussed above, acts as significant barriers in the growth of cloud computing. Among them security and privacy of data and applications are the major rising concerns. Now the focus is on security issues related to cloud computing that is discussed next.

1.4 Security in Cloud Environment

In cloud computing paradigm, a cloud provider creates, deploys and manages the resources, application and services depending on the provider being IaaS, SaaS, or PaaS. Multi tenancy and virtualization are the key features to make efficient utilization of the existing resources and applications. A single server, computing facility, data center and operating system hosts many users by using virtualization. A large number of users are getting served by a cloud provider by this concept of resources sharing. Data protection, communication, resource management for isolation and virtualization are some of the security issues arising due to multi-tenancy and
virtualization in the cloud environment. Major types of security threats in the context of cloud application are captured in figure 1.1 and briefly described below.

Figure 1.1: Classification of Security

1. **Data Protection:** The cloud computing infrastructure is shared among multiple users at any point of time. User data is stored and processed in a shared environment that is under provider’s control. User data may be tampered with by other malicious entity. Lack of transparency about the data storage location in the cloud environment, regulatory issue due to cross border storage, etc. makes the requirement of data privacy and protection in cloud environment more prominent. Thus data protection issues including data confidentiality, integrity and availability are key security issues in cloud computing.

2. **Application Security:** Application software running on or being developed for cloud computing platforms presents different security challenges. Application that is running from the remote should be from authentic provider and without malware. Flexibility, openness and public availability of cloud infrastructure are threats for application security. Preserving integrity of applications being executed from remote machines is also one of the concerns.

3. **Network Security:** A cloud computing can be of type public or private, based on the deployment model. Service and applications are accessed from remote locations in a cloud environment. Continuous availability of cloud service without any disruption due to network security problems like denial of service, and other attacks are important security challenges.

4. **Virtualization Security:** Virtualization technology introduces possibility of new attacks through the hypervisor and other management components. There is no reliable means to assess security of Virtual servers and applications. Multi-tenancy in cloud infrastructures for sharing
physical resources between VMs (Virtual Machine), can give rise to man-in-the-middle attack at the time of authorization for any service. VMs are created and revert back as and when needed in the cloud environment. Because VMs can quickly be reverted to previous instances, and easily moved between physical servers, it is difficult to achieve and maintain consistent security. Therefore virtualization security is a concern while using the cloud resources.

5. Identity Management: Identities are generated at the time of registration process for cloud services to access it. Each user uses his identity for accessing a cloud service. Unauthorized access to cloud resources and applications is a major issue. A malicious entity can impersonate as a legitimate user and access a cloud service. Many such malicious entities acquire the cloud resources leading to un-availability of a service for legitimate user. Also it may happen that the user crosses his boundary at the time of service usage. This could be in terms of access to protected area in memory or performing any operation that are not maintained in Access control List for a specific resource and application. Thus Identity Management system for providing authentication and authorization is an issue for both provider as well as user in a cloud computing environment.

All these security issues in cloud environment are active areas of research and experimentations. Various issues discussed with respect to cloud security are analyzed. Lots of research is going on to address issues like network security, data protection, virtualization and isolation of resources etc. Many solutions exist and many are evolving. The thesis focusing on measuring and evaluating the security “trust” of the various methods provided for addressing security issues in cloud computing by a specific cloud provider and for a given service.

1.5 Problem Definition

Many cloud services are available in the market with their specifications and features. Security concerns for services are major criteria for users to select one amongst the available based on their requirements and demand. A cloud user who want to select a particular service based the security issues addressed by the providers, requires some tools or ranking service for cloud service evaluation. A framework which evaluates the security of cloud services is the demand by cloud users to select a particular service based on their security needs. Thesis is focusing on the security strength evaluation of the cloud services.
The focus here is on a framework for such an evaluation of service security in a cloud environment. Such a framework should identify the techniques for providing security in a cloud computing environment to be evaluated and ranked. Security of a cloud service should cover many aspects like authentication, authorization, data protection etc. These are the basic security goals which constitute principles of security and become crucial while moving on towards the cloud. Therefore a tool that assesses and evaluates these security concerns with respect to cloud services before selection is the necessity in the cloud environment.

Here a trust model is proposed that is used to evaluate cloud service security strength. It consists of a trust value that is overall security strength of the cloud service. Model includes a list of parameters that covers almost all relevant aspects of security. A trust based evaluation is formulated to evaluate trust value. A list of such parameters is identified. The evaluation procedure and formulae are identified to calculate the overall trust associated with a cloud computing application and service. The set of parameters and their formulae will form a trust model for a cloud service or application. The formulation of such a trust model in cloud computing environment is the outcome of this research.

The trust value calculation discussed so far gives static value. As the service is used by many users and multiple times, associated parameter values may change. Value of trust is affected, based on user experience and transactions over a period of time. A more refined trust value called dynamic trust can be evaluated which can increase or decrease with respect to the previously calculated or static trust. Dynamic trust is required for getting the updated value of trust over a period of time.

Further implementation and simulation environment for validating trust value in a distributed environment will be required. The model is validated and its adequacy is checked with respect to existing cloud services. The trust value obtained by the model gives the overall trust for the existing services at various levels of security considerations.

Finally an infrastructure and framework will be presented where the trust values are calculated both statically and dynamically. Various services that are available in cloud environment can be evaluated for trust values. A reputation and trust management system will be given to compute the reputation about the cloud providers and their services.
Thus trust model acts as a security strength evaluator and ranking service for cloud application and services. It can be used as a benchmark to setup the cloud service security and to find the shortcomings and improvements in cloud infrastructure.

1.6 Thesis Overview

The rest of the thesis is organized as follows. Chapter two covers detailed literature survey where important aspects of security issues in various collaborative environments are considered. The various cloud security issues and corresponding solutions from the literature is analyzed and summarized at the end of the chapter. Chapter 3 deals with the proposed trust framework starting with the trust model. Model is detailed with the different parameters in this chapter. Chapter 4 describes extending this model into a dynamic trust model with a set of dynamic parameters. Chapter 5 discusses implementation of the cloud computing test-bed. Accuracy and validity of the trust model is analyzed in chapter 6. Finally conclusion and future scope as chapter 7 ends the thesis.