Chapter 10
Cloud Computing: Security Concerns and Issues

Shantanu Pal
The University of Calcutta, India

ABSTRACT
In a cloud ecosystem, most of the data and software that users use reside on the remote server(s), which brings some new challenges for the system, especially security and privacy. At present, these security threats and attacks are the greatest concern for the service providers towards delivering a more secure cloud infrastructure. One of the major concerns is data security, implemented by the most effective means possible and the protection of stored data from unauthorized users and hackers. When considering these security issues, trust is one of the most important means to improve the system's security and enable interoperability of current heterogeneous cloud computing platforms. The objective of this chapter is to discuss and understand the basic security and privacy challenges of a cloud computing environment as the security of cloud computing is the greatest challenge for delivering a safer cloud environment for both the service providers and the service customers. With this in mind, this chapter will introduce the risks and possible attacks in a cloud computing environment. The major goal is to specify the security risks and attacks and consider trust of cloud service users for delivering a safer and innovation business model.

INTRODUCTION
Nowadays computer computation has changed immensely. In recent years, the term Cloud has emerged rapidly over the Internet towards faster and more innovative business environments. From the small investor to the big IT (Information Technology) companies, many of whom are now relying on this system. Cloud has several advantages such as its ease of use and maintenance, the relatively low power consumption, unlike other systems and the reductions in overhead for storing and servicing data for companies. However, in spite of these advantages cloud also suffers from different security threats and attacks.

When we sit in a car and start it we don't analysis what is going on under the hood of the car. We do not think about how the motor starts nor are we concerned about the services provided...
that work the mechanics of the car such as the lights or the brakes or even the radio. We may not consider how the accelerator works or how it causes the vehicle to move fast or slow when we push on or release the pedal. The same thing is going on in the modern computing environment, where we only need the services according to our choices and financial supports available for it. These new type of paradigms are known as Cloud Computing.

In 1969, Leonard Kleinrock said (Buyya, Pandaey, & Vecchiola, 2009): “As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of ‘computer utilities’ which, like present electric and telephone utilities, will service individual homes and offices across the country.”

In recent years, the term cloud has gained remarkable popularity due to the economical and technical benefits provided by this new way of delivering computing resources, and the pervasive availability of high-speed networks. Businesses can offload their IT infrastructure into the cloud and benefit from the rapid provisioning and scalability. This allows an on-demand growth of IT resources in addition to a pay-as-you-go pricing scheme. This scheme does not require a high up-front capital investment for setup a cloud infrastructure for their businesses. These benefits are in particular more attractive to small industries/business that prefer to avoid intensive up-front capital investment for their IT infrastructure. However, the benefits of cloud computing is not limited to such small business, from governmental services to defense sectors is deploying their services into cloud platform. These general principles of cloud computing can be implemented on different abstraction levels. While Infrastructure as a Service (IaaS), such as Amazon EC2, provides virtual machines, storage and networks, higher abstractions include Platform as a Service (PaaS) and Software as a Service (SaaS) that provide the actual Web-based applications to the end-users (Cloud Service User or CSU).

In a cloud computing environment, most of data and software that users use resides on the one or more remote server(s), which brings new challenges for the system, especially security and privacy. One major concern is data security, and the most effective ways to protect these sensitive data from unauthorized users and hackers. When considering these security issues, trust is one of the most important means to improve the system’s security and enable interoperability of current heterogeneous cloud platform. To date there are several security and trust mechanisms has been proposed to deliver a more secure cloud based application, but many of them are not effective enough to prevent the unauthorized users accesses of the cloud data and also to reduce vulnerabilities in a cloud computing application.

The rest of the chapter is organized as follows: very fist a brief discussion of cloud computing is made to understand the basic architecture of present heterogeneous cloud environment. Then advantages and disadvantages of cloud computing is discussed. Issues, service layers, mode of cloud computing and virtualization are also briefly discussed. Difference security risks and attacks, threats and storage security in cloud data are broadly discussed in this chapter. A view of cloud market orientation is also presented. Finally, the chapter ends with a brief conclusion and future direction.

SECURITY IN CLOUD COMPUTING

Cloud computing is the result of combining Service Oriented Architecture (SOA) and Internet Technologies, mainly Web services and virtualization (Brock & Goscinski, 2010). While cloud computing has made resources accessible to the end users, this technology made resources vulnerable (primarily from sharing same resources and virtualization) for different security threats and attacks. Research is ongoing for the improvement of performance, reliability or scalability in