Technical survey on cloud computing and its security issues

ABSTRACT

Cloud computing also referred to as “Cloud” is one of the most growing branches of Computer Science. It has helped in storing and accessing data resources remotely over the Internet. This technology uses shared resources instead of storing resources individually on each computing machine. It offers several benefits such as anytime access, low cost, scalability, convenience and availability. Despite having many features, cloud computing has some issues too. The most critical issue of Cloud Computing is its security. The security risks and privacy issues are higher when data is stored on individual machines compared to the data stored on “cloud”. These risks have to be considered by customers before moving to cloud service. In this paper, we have discussed the definition of cloud computing, its categories (IaaS, PaaS and SaaS), several clouds computing security issues and solutions against cloud computing security problems.

Keywords— Cloud computing, Cloud security, DES, TDES, Message digest

1. INTRODUCTION

Cloud Computing is a technology of computer science that is based on a computer network and focuses on sharing resources using the Internet. Many renowned companies such as Google, Facebook, Amazon, Microsoft, Yahoo and several others have been working hard to develop more and more cloud computing systems and also improving their services to reach a plethora of users across the globe. However, many clients are still reluctant to switch their businesses to the cloud server because of the security and privacy issues involved with cloud computing. In cloud service, clients only pay for the services they choose and do not pay for resources like infrastructure or storage devices. There is three type of cloud environments available – Public, Private and Hybrid. A public cloud is a model that is available to the general public and can be used by people to access data online and store their data. Public Cloud maybe free or not free to use depending on the hosting service. Private Cloud is not available publically and can be only used by the people who have authorized access to it. Private Cloud is commonly secured and requires authentication. Public Cloud and Private Cloud when combined, form the Hybrid Cloud model. In this service, some data is accessible by the public while some have restricted access. Cloud computing is further divided into three major categories: IaaS, PaaS and SaaS [1].

2. CLOUD COMPUTING

Infrastructure, Platform and Software as a Service are the three main models of Cloud Computing which are accessible over the Internet. These services are given to users as pay-what-you-use where clients pay only for the services that they opt for a given time unlike services like file hosting, web hosting etc. The pricing of cloud services also changes depending on the Quality of Service needs. The Cloud models are classified into Public, Private and Hybrid Cloud where public cloud is available to the general public and private model is only accessible by authorized users. Some of the Cloud Computing platforms are Amazon EC22, Microsoft Azure and Google App Engine.

People often treat Grid Computing and Cloud Computing as same while they are different technologies. In order to get rid of this confusion, this section lists the characteristics and definitions of Cloud Computing.

2.1 Characteristics of cloud computing

One needs to understand the features of Cloud Computing in order to differentiate it from other network services. Characteristics of Cloud Computing given by Literature [2] are: Cloud Computing (a) ensures reliability and data security. Users are no longer afraid to lose their important data or information and their data is also protected from virus and other attacks. (b) Available Low Cost since it offers its clients to pay only for the services that they use and opt for. (c) Easy to understand and use for new users. Its features
given by Literature [3] are Separate space and storage for software and important files like system program, data and library files over the Internet. Services provided for users can be used on a user terminal or compute server. From the above characteristics, the main features of Cloud are paid as you use and remote usage of resources and data files.

2.2 Definition of cloud computing
One of the rising technologies of IT industry is Cloud Computing. It doesn’t have one accepted definition. Many institutions and researchers have given their own definitions. The Literature [4] gives the definition as Large dataset of resources that is easily accessible and usable which can be stored on the cloud for using resources effectively and prevents duplicate data. The National Institute of Standards and Technology Bureau described it as The technology that permits its customers to fetch information like a server, applications, and files without service providers’ involvement. It has five important features: on-demand service, remote access, rapid elasticity, resource pooling and measured service.

2.3 Cloud service models
In the current scenario, almost every company, internet service providers have started providing cloud services to their users. As said above, Cloud Computing can be further divided into three Service Models: IaaS, PaaS and SaaS, as shown in figure 1.

![Cloud service models: Top service has the best development](image_url)

(A) **Infrastructure as a Service (IaaS)**
Infrastructure as a service-institutions, companies or general public use the cloud to access the data available online which includes files and applications. It is identical to Utility computing which provides the services that the user has paid for. SaaS and PaaS services rely on IaaS for getting computing power without paying the extra cost. Using Cloud service providers can gather storage, I/O devices and more, together in a large pool of dataset for providing services to clients, SaaS and PaaS.

(B) **Platform as a Service (PaaS)**
It is a type of cloud computing service model in which hardware and software applications are offered to users over the cloud. It frees customers from installing hardware or software onto their systems for running a new application. Some PaaS providers charge money for these services. The user only needs to pay for the services that they opt for. Some common PaaS providers are Red Hat OpenShift and Google App Engine.

(C) **Software as a Service (SaaS)**
It is a type of cloud computing service model which facilitates its users by providing software over cloud so that individuals do not have to install software on individual systems. The user does not require to install any hardware. This service is purchased on a subscription basis. This service keeps the software updated all the time without user’s interference. It is also referred to as On-Demand Software.

3. CLOUD COMPUTING SECURITY ISSUES
When we talk about Cloud, there is a number of security issues and concerns associated with cloud computing. Security issues are classified into two divisions. First is security issues faced by cloud providers. Software, platform or infrastructure as a service through cloud are provided by cloud providers. Safeguarding client’s data and applications and providing a defence mechanism to ensure that infrastructure is secured is the provider’s top priority. Second is Security concerns faced by customers or clients. Customer must ensure that the provider has taken security measures to protect their information. Some think that in the cloud era, data and applications are stored in the "cloud" and public cloud provider or private cloud provider offer technical support, so the centralized control management is helpful to information security. Exhaustive security protection is provided through the deployment of centralized cloud computing. However, the centralized management of a cloud computing centre is prone to hacker attacks conjoined with magnitude system and complexity.

Security problems associated with cloud system are in the following five aspects:

(A) First, increased security attacks due to the immense amount of user data stored in a cloud system for attackers. If an attacker is able to bypass the security mechanism, it can lead to loss of control for both cloud providers and users. On the other hand, the cloud system provides users with more open access to provide greater flexibility.
Second, newly peculiar security concerns for customers of public cloud service have been generated due to too much use of virtualization in implementing cloud infrastructure. The connection between OS and I/O components is changed by Virtualization. The hardware could include computing, storage and networking. Since the virtualization layer is controlled by a central management console, specific mandatory actions must be taken to secure virtualization software without compromising the integrity of data. For example, a breach in the administrator workstation of virtualization software can lead to whole data system go down or reconfigured.

Third, Loss of control when data remain in the cloud even after termination of the contract. Data encryption and Tokenization are key solutions to this problem.

Fourth, ensure the integrity and privacy of user data: The primary purpose is to get user privacy, and then to obtain economic benefits. In this case, relevant laws and regulations should be enforced and to protect third-party security, to meet requirements listed by companies, especially to clear responsibility division when problems arise and to offer safeguard mechanisms as cloud service providers terminals. Most enterprises are reluctant to store sensitive information in third-party, and they still focus on building a private cloud.

Fifth, ensure continuity of the cloud platform services and high availability of user data and business. Cloud computing service needs to provide a fault tolerant mechanism to backup user data to decrease the impact in the application when the real data is destroyed. Also, the software itself may have loopholes and a large number of malicious attacks happen, which can greatly increase the possibility of service interruption.

SOLUTIONS AGAINST CLOUD SECURITY THREATS

There are several solutions available to prevent unauthorized access and breaching of security. Verifying access control by setting up data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by the cloud service consumer. The cloud service provider must ensure that only authorized users can access the consumer’s data. Even the best security protocols in the cloud can be cancelled by an unauthorized user by a loss of endpoint device. The accessibility of data to only authorized user or client must be ensured by Cloud service providers. Most providers do not offer the neutralization of data from drives each time the drive space is abandoned. Insist on a secure deletion process and have that process written into the contract [5].

SECURITY MECHANISMS

To ensure that the data is kept out of reach of unauthorized people, encryption of data plays a vital role in the real-time environment, such that it is not mutated and breached and sending in a different format is a most protected way to transmit the data through the network.

5.1 Encryption Algorithms

5.1.1 Data Encryption Standard (DES): The cryptographic algorithm used widely nowadays is the Data Encryption Standard algorithm. It is a symmetric block cipher technique and uses the same binary key to encrypt and decrypt data blocks. It was created by IBM, approved by the NSA. It operates on 64-bit data, processes it under a 56-bit key. It uses a sequence of primitive operations called round to encrypt a data block-16 rounds are used.

5.1.2 Triple DES (TDES): Triple-DES uses symmetric key block cipher. DES cipher algorithm is used thrice on each data block. It provides a relatively simpler methodology to increase the key size of DES. Triple DES uses an encrypt-decrypt-encrypt process. It provides better security than DES however it is slower.

5.1.3 Message Digest: A message digest is a fixed size numeric representation of the contents of a message, computed by a hash function. It can be encrypted to form a digital signature. Messages are mutable in size. The message is sent along with the message digest. When two message digests are the same then the verification of the integrity of the message is done [6].

CONCLUSION

Cloud Computing, just like other technologies these days has been able to reduce the cost of previously available technologies. Every technology has its pros and cons, while the cloud offers so many features to its users, it also has some issues related to privacy and security. These security issues can be dealt with by using the above mentioned cryptographic security algorithms, to provide clients secured and reliable environment to store and access their data.

Cloud service providers usually have highly configured powerful servers to offer uninterrupted and best service to its customers but the cloud is always a risk just like other network-based technologies. This causes the users to just store less important data on cloud servers and the rest on their local machines.

To summarize, although Cloud Computing is an interesting and useful technology, it doesn’t mean that all individuals, institutions and companies should switch to the cloud. One should first consider several factors like reliability, performance, scalability and most importantly Security of Data before switching to cloud services.

ACKNOWLEDGEMENT

We thank Mrs Shikha Rai (Assistant Professor – Department of Information Technology) for providing assistance, support and time in the preparation of the manuscript. Her critical and helpful comments on the early draft helped us throughout the research paper. We would also like to thank our friends and family for their constant support.
8. REFERENCES


