RESEARCH ARTICLE OPEN ACCESS

Survey Paper on Basics of Cloud Computing and Data Security

Jasleen Kaur[1], Ms.Anupma Sehrawat[2], Ms.Neha Bishnoi[3]

Research Scholar[1], Lecturer[2 & 3],
Amity University, Gurgaon
Haryana- India

ABSTRACT

Cloud computing is a type of computing that is based on the internet. It provides various hosting and delivering services over the Internet. It provides the computational resources (Server, Storage, OS and Network) to user as service, based on the demand of user. Cloud computing has gained its popularity by providing cheap and easy access to IT (Information Technology). However, despite the fact that demand for cloud based resources is increasing day by day but on the other side security is regarded as a serious issue on which work has to be done. In this paper, we present a survey of cloud computing, highlighting its key concepts, architectural principles, deployment models, service models, benefits as well as security issues related to cloud data. This paper also discusses the related work done regarding security such as Playfair cipher, Proxy re-encryption and Railfence technique. The aim of this paper is to provide a better understanding of the cloud computing and to identify important research directions in this field.

Keywords:- Cloud Security, Proxy re-encryption, Playfair, Railfence

I. INTRODUCTION

Cloud Computing simply means storing and accessing data and programs over the internet instead of computer's hardware. It provides developing environment, ability to manage the resources, application software over the cloud [12]. It provides resources to customers on a pay-as-you-use basis. Users can access the services available on the cloud by having an internet connection. Many companies are delivering services from the cloud. Some examples are:

A. Google — It has a private cloud that offers online productivity software including email access, document applications, text translations, maps, social networking google+ etc.

B. Microsoft — It provides online service that allows the tools which are required for business purpose are moved into the cloud[17], and Microsoft currently makes its office applications available in a cloud which includes online storage, file sharing, website design and hosting..

C. Salesforce.com — It allows us to deliver revolutionary customer service from anywhere, anytime on any device.

II. CLOUD ARCHITECTURE

Cloud Computing architecture consists of various components, front end, back end, cloud based services such as saas, paas, iaas and an internet connection. Front end comprises of clients, mobile devices which provides access for the cloud computing system. Back end comprises of the storage servers, virtual machines, security mechanisms. Each of the ends is connected by internet connection.
The whole system is in the hands of central server and it is also used for controlling and managing clients demand and traffic [11]. For the communication of computers that are connected in a network "Middleware" software is used.

III. USING THE CLOUD

Through an internet connection we can access our information from any place at any time from the cloud. While in a simple laptop and simple computer it is required that we should be at the same location where our data is present [8], but in the case of cloud computing there is no need to be at same location. Users simply need to log on to the network and can use the services of the cloud.
Internet connection is the basic requirement in order to access the cloud. Internet connection can be established through a wireless or wired internet or through a mobile broadband connection. We can use type of cloud and type of service offered according to our requirements. We can use it as on rental basis.

IV. DEPLOYMENT MODELS

There are different types of clouds that one can subscribe to depending upon their needs.

***A. Public Cloud*:** A cloud in which service providers made their resources available to the general public. It provides economy of scale as infrastructure cost is spread to all users. It provides more scalability and efficiency in shared resources.

B. Private Cloud: A private cloud is established for a specific group or organization and limits access to just that group [8]. It offers the highest degree of control over performance, reliability and security.

C. Community Cloud: This cloud infrastructure is shared among a number of organizations with similar interests and requirements [1]. The goal of this cloud is to have the benefits of public cloud with more privacy and security.

D. Hybrid Cloud: A hybrid cloud is a combination of two or more clouds. As it is the combination of models, it offers the advantages of multiple deployment models. It provides ability to maintain the cloud as recovery of data is easy in this cloud. It offers more flexibility than both public and private clouds.

V. SERVICES PROVIDED

There are three types of cloud services provided by cloud for subscription: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three types provide different services for the cloud. Choose the provider according to the needs and services provided.

A. Software as a Service: SaaS is a software delivery method which provides access to application hosted by service provider. Users no need to license the software and don’t need to invest in hardware [16]. Examples of SaaS providers include Salesforce.com

B. Platform as a Service: PaaS refers to providing platform which includes operating system support and software development frameworks where the organization can create its own custom applications for use. Examples of PaaS providers include Google App Engine, Microsoft Windows Azure and Force.com.

C. Infrastructure as a Service: IaaS Consumers control and manage the resources according to customer needs in terms of the operating systems, applications, storage, and network connectivity.

VI. BENEFITS OF CLOUD COMPUTING

A. Expand scalability: It provides on demand scalability. User can meet his changing requirements with this capability of cloud computing. It can scale up resources and manage them.

B. Less infrastructure costs: It provides service of pay as use basis, so there is no need to invest in the infrastructure cost. Organisations owned memory and resources according to their needs.

C. Increase utilization: Multiple clients can share computing power, with this utilization is increased in cloud computing [10].

D. Improve reliability: As data is stored in the cloud, Backing up and restoring of data is easier than on a physical device.

E. Easy reach to resources: Cloud offers more advanced tools that smaller organizations were not able to approach earlier. These tools are accessed with an internet connection.

F. Easy accessible: After registering in the cloud one can have access to the information from anywhere and any time with an internet connection.

VII. SECURITY IN CLOUD COMPUTING

Data security

According to the survey through previous papers, Data security is regarded as an important research topic in cloud computing. The major issues related to data security include data integrity, data availability, data confidentiality, transparency of data [6] and control over data where data resides. There are various aspects for providing data security such as by providing access controls and encryption methods. The service provider must be ensuring that their infrastructure that providing is secure and client’s data remain protected [15].

On the side of client, they should look into the security measures related to data that what are the security techniques are provided by cloud provider. Techniques provided are the choice of cloud provider. Techniques comprise of various encryption methods like various algorithms are there such as AES, RSA [9] etc. As data is stored in the cloud, there is threat to the data from the unauthorized user. To prevent this access control mechanisms should not be ignored [13]. Cloud provider should provide authentication method which checks the authenticity of the user to prevent threat to critical data. There are various authentication schemes such as SSL, PKI, CHAP which checks authenticity of the user [14]. After authentication, authorization can be provided which limits the access of the user.

VIII. PRACTICES FOR CLOUD SECURITY

A. Secure access

Usually users access the cloud using client web browser. Make sure browsers are properly updated and protected from browser exploits. By using this, data can be prevented from threat to some extent.

B. Backups and restoration

There should be proper mechanism provided by the service provider so that customer is able to have backups of the cloud based resources and data. Some services like Amazon S3, Amazon Dynamo DB provide automatic data restoration [7].

C. Data Integrity

To ensure data integrity, limits the area of use of resources for users [2]. This can prevent the modification of data and hence data integrity is maintained. In case data integrity is enforced restore the data from backup with the help of backup services provided.

D. Encryption of data

Data encryption provides protection to the data. Encryption should be done before the data is moved to the cloud [4]. If an unwanted user wants to access the critical data, encrypting the data makes it much more difficult for unwanted user to do anything with wrong inception.

E. Evaluation

Evaluate applications, business processes and data according to their value and risk associated with them then create cloud with precautions and tools to make the cloud secure.

IX. RELATED WORK

A. Proxy Re-Encryption Schemes

During a proxy re-encryption scheme, a proxy server will convert the plain text to cipher text under a public key PKA [3] and then this cipher text is again encrypted under another public key PKB by the re-encryption key RKA->B and in this way plain text is transformed into cipher text. In this scheme, messages are encrypted before storing into the storage server. If a user wants to share his messages, he sends a re-encryption key to the storage server. The storage server has the encrypted messages and then it re-encrypts with the re-encryption key for the demanding user. Thus, their system has information confidentiality and secure way of communication.

B. Playfair Cipher

It contains a square matrix of 5X5 alphabetical letters arranged in an appropriate way [5]. In matrix key is placed by the user by selecting the key [5]. The remaining letters are then placed one by one from the key in the matrix. Different pairs are made by breaking plain text into pairs. If a pair contains same alphabet then they are separated by introducing a letter "x". Otherwise if the pair having different alphabets and located in the same row of matrix then there is replacement of each letter with letter ahead of it. If the pair is in same column of matrix then there is replacement of letter with letter below it and when the pair of letters is neither in same column nor in same row then they are replaced by the letter in their row that resides at the intersection of paired letters.

C. Rail fence technique

It is one of type the transposition ciphers, in which plain text is written as a sequential diagonal form and during cipher text it is read as row by row [5]. For example, the message "how is you" with a rail fence of depth 2 is written as,

```
 h w r y u
    o a e o
```

Now the message is read as "hwryuoaeo". Hence the message is changed to encrypted form and it cannot be understand by unwanted user.

X. CONCLUSION

To summarize, the cloud provides many services for computer user as well as large and small organizations. It covers area of computing to a broader range and increases the ease of use by just having access through any internet connection. However, despite of this it also have some weak area to work upon. Through survey security is regarded as the weakest area. Various security mechanisms are implemented in the form of encryption algorithms. Encryption algorithms do not provide authentication check for the user. Authentication method should be deployed to the cloud to provide authenticity of the user.

It is the duty of cloud provider to protect the cloud against the security threats. If we want to use the services of the cloud, check for the methods provided for the security purpose. We should choose the type of cloud and the type of provider according to our needs that will be most useful to us.

REFERENCES

[1]. Mandeep Kaur, Manish Mahajan "Using encryption Algorithms to enhance the Data Security in Cloud Computing", "International journal of communication and Computer technology", Volume1, Issue3, Jan 2013

[2] Dr.A.Padmapriya, P.Subhasri, "Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", "International Journal of Engineering Trends and Technology (IJETT)", Volume4, Issue4-April 2013

[3] Aarti P Pimpalkar, Prof. H.A. Hingoliwala , 'A Secure Cloud Storage System with Secure Data Forwarding', "International Journal of Scientific & Engineering Research",Volume4,Issue6, June-2013, page no-3002-3010

[4] Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", "International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)",Volume2, Issue 7, July 2013

[5] L. Arockiam1, S. Monikandan, "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm", "International journal of advance research in compute rand communication engineering", Voumel2, Issue 8, August 2013

[6] Anitha Y , "Securiy Issues in cloud computing", "International Journal of Thesis Projects and Dissertations (IJTPD) Vol. 1, Issue 1, PP: (1-6), Month: October 2013

[7] Jinesh varia," AWS Cloud Security Best Practices","White Paper", November 2013

[8] Alexa Huth and James Cebula,"Basics of cloud computing", "United States of emergency leading teams",2012

[9] Parsi Kalpana ,"Data security in cloud computing using RSA" , International Journal of Research in Computer and Communication technology,ISSN 2278-5841, Volume 1, Issue 4, September 2012.

[10] Vmware, "Securing the cloud, A review of cloud computing, security implications and best practices"
[11]Miklau and D. Suciu, "Controlling access to published data using cryptography," in Proceedings of the 29th international conference, 2011, page no- 31-46

[12] Luit Infotech Private Limited,"What is cloud computing"

[13] H. Narayanan and M. Gunes, "Ensuring access control in cloud provisioned Healthcare systems," in Consumer Communications and Networking Conference (CCNC), 2011, page no-.247–255.

[14] Chittaranjan Hota, Sunil Sanka, Muttukrishnan Rajarajan,SrijithK.Nair,"Capability-based Cryptographic Data Access Control in Cloud Computing", "Int. Journal of Advanced Networking and Applications" Volume: 03; Issue: 03; Pages:1152-1161 (2011)

[15]Qi. Zhang ·Lu. Cheng, Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", "The Brazilian Computer Society", April 2010

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010, page no- 1–9.

[17] http://en.wikipedia.org/wiki/Cloud_computing

IJCST