RESEARCH ARTICLE OPEN ACCESS

A Systematic Analysis Of Cloud Computing: A Review

Bisma khanam[1], Dr Parul Agarwal[2]
1Computer Science and Engineering, Jamia Hamdard university, New Delhi
2 Computer Science and Engineering, Jamia Hamdard university, New Delhi

Abstract:

Computing has come from the long way that is evolved from parallel to distributed to grid and now to cloud computing. To store data and to perform various tasks a vast infrastructure is provided by cloud computing. It becomes necessary to secure this huge data on cloud. One of the promising field that have emerged in Cryptography is DNA Cryptography. This technology is used in many fields and can used to solve many large problems. For cloud security DNA cryptography can be used to optimize data security. To secure communication on the cloud DNA cryptography is used. This paper presents survey of different techniques utilized by various researchers to use DNA cryptography for cloud security.

Keywords **— Cloud computing, DNA, Cryptography, plain, text, cipher text, Encryption, Decryption.**

I INTRODUCTION

Cloud computing revolutionized the IT industry. On the top of virtualization and abstraction cloud computing is built. Various features that cloud computing is having are: Data availability, Multi-tenancy, effective pricing, Data integrity, Services on demand. In cloud computing at the time of need users can request resources. This technology is fully dependent on the internet in which data of the data of the user can request resources. This technology is fully independent on the internet in which data of the user is stored and is also maintained by the cloud providers like Amazon, Microsoft, Salesforce.com, and Google. The service that is done in the technology of cloud computing and is provided to user over internet is known as cloud services. Hard drives and local storage devices can be avoided as cloud storage provided with a privilege to store even files to remote databases. Cloud computing can also be considered in light of fact whether the data to be accessed is found or not in cloud. It is proved that as far as device has access to web, it can access data for anytime and even run software program in it also no specific place is required for accessing data even can be accessed remotely anytime anywhere. It can be said that internet turned out to be cloud and all the information and applications accessible to any device that can be associated to internet anywhere in world. Companies had empowered their users with the help of cloud services to access files remotely that are stored on remote areas via the internet connection[14]. Better explanation of cloud computing is that it provides shared resources depending on the customer demands. Some characteristics of cloud computing are

- Efficient utilization of the cloud infrastructure because of the sharing of resources and costs among large number of users is possible.
- Multiple sites that well suited the continuity of business and help in recovering disasters can be used for obtaining reliable services. However at times a number of services provided by cloud suffers from disruption and at those events consumers cannot do anything.
- Maintaining cloud computing applications is very easy as installation on every user's computer is not needed.

- The use of cloud services show transparency to user and service supplier that utilizes the service as they can be measured. Metering capability of cloud computing services helps to control and optimize resource use[15]. It resembles the way air time, concerning water and electricity for cities, and also information technology services are charged by the amount as per their usage.
- Cloud computing provide the security that is good in comparison to the security provided by traditional systems as the providers have the power to provide resources that can solve security issues which may customers cannot afford. However, in case of quite confidential data security remains the main concern/issue in cloud.

Various features of cloud computing are:
On demand self service: In this feature the user of the cloud service can request for the resources from cloud service provider and they have to control these resources on their own as there is very less interplay between the user and service provider.
Broad-network access: Services that are provided by the cloud service provider over the network that is rented from the private service providers or internet and these services can be accessed by making use of devices such as pen-drives, phones, and laptops over the interfaces with the network access.
Resource pooling: Various resources are taken together into pool and these resources are then shared with many users from the remote location. This can be done by using model that is multitenant in the opinion of the user's needs by dynamically allocating regaining resources that ranges for individual elements to the complete machines.
Rapid elasticity: The need for the resources can increase or decrease according to business needs to meet the requirements in the work. Example of elasticity in an education field would be at time of announcing of result for examinations in state or country where millions of people will request for the result at the same time from the server.
Measured service: The services that users use are measured and according to the usage bill is provided. The services that are rented are also properly monitored, controlled, reported, and allocated. The billing of these rented resources is done either monthly, per day, or on the basis of hours.

Benefits of cloud computing

Some of the advantages or benefits of cloud computing are:-

- Less infrastructure cost: The need for large number of devices are not required, therefore staff is not needed to maintain these devices. Thus leading to less cost for infrastructure.
- Cost for maintenance is low: The hardware and software for cloud is maintained by service provider only. User doesn't need to maintain, so reduces cost for maintenance.
- Reduced cost for software: The consumer doesn't need to buy license to install the software in all the computers in the organization and for updating the same. This reduces the software cost.
- Automatic software updates: The software that is rented by the customer is automatically updated by the service provides whenever it needs new update[12]. This automatically update is done according to the preference of the consumer.
- High reliability and availability: The services that are rented by the user are all time available. If there is any failure in the service providers immediately detects the failure and corrects the failures
- Pay-per-use-model: The services that are used are metered and bill is paid according to the utilization.

Cloud service models

Depending on needs of users any type of cloud service can be used. The primary services provided by the cloud are:

Software as service (SaaS): is a model for software distribution in which different resources are provided by service providers and are made available to the users through internet. SaaS can also be called as "on demand based software". Various applications provided by SaaS are customer relationship management (CRM), DBMS, games, financial, and accounting application to the customer as service. By using cloud customer doesn't need to provide huge amount[11]. Users need to pay as per the usage.

Platform as service (PaaS): is a type of cloud service delivery model which gives platform for computing and solution as a service. Various computing platform that are provided by PaaS as service are programming language, operating system, runtime environment, compilers. This service model is beneficial for the developers of applications, run, and test applications with no need for configuration and management of platform and deployment and development

Infrastructure as a service (IaaS): IaaS is one of cloud service delivery model providing infrastructure for computing consists of security, networking, operating system, and servers for the development of applications and for deployment of databases., tools etc as a service. The services provide of IaaS are network resources, storage devices, load balancers, firewalls etc. The providers of services provides services on demand, they take resources from the pool, and provider to the end users.

Cloud deployment models

The important task to deploy a computing answer of cloud is to come to conclusion about the kind of cloud that is to be applied. Different kinds of cloud deployment that currently took place are public, private and hybrid clouds.

Public cloud: The services are provided to the public and the service provider maintains the cloud infrastructure. Public can be any one like small or big organization, an individual. Users are allowed to access to the public cloud through the usage of web browsers via interfaces. Pay per use service is provided to the user that is user has to pay only for the time period it has used the service.

Community cloud: The cloud infrastructure shared by the number of organizations for fulfilling their requirements comprises of community cloud. The members of the community cloud may be many individuals or organizations.

Hybrid cloud: Hybrid cloud can be defined as the combo of private and public cloud. For this case one or more external services are linked to private cloud. Hybrid cloud helps organizations in serving their needs in private cloud and sometimes asks public cloud for the computing resources.

DNA stands for Deoxyribo nucleic acid that stores information related to the features of an organism. Every individual have unique DNA. Every nucleotide is composed of Deoxyribo sugar, nitrogenous base, and phosphate group. Nitrogenous bases is composed of Purine (adenine and guanine) and pyrimidine (cytosine and thymine). A and T and between G and C bonding is present. There is important role of this bonding in DNA cryptography. One of the emerging technique is DNA Cryptography. In this technique, the data is converted into the various combinations of A,C,G and T that form the human deoxyribonucleic acid (DNA).

II Security issues in cloud computing

Loss of confidentiality and integrity are the major security issues in cloud computing. The network that is used to connect cloud should be secure and mapping should be done securely. Various security issues in cloud computing are:

I. Access To Servers And Application

Data access is mainly related to security policies provided to the users while accessing the data. Atjus it becomes necessary to restrict the access of data and keep eye on the access in order to check the changes that are made in system.

II. Data integrity

Integrity means that data is transmitted same as the sender sends the data. So in case of cloud computing to maintain integrity is very important. ACID (atomicity, consistency, isolation, and durability) properties should be followed in order to maintain integrity. ACID transaction is supported by most databases and they provide integrity of data.

III. Data Location

In general, cloud users doesn't know where data is stored in data-centers and there is no command over the physical access to that data. Data-centers of the cloud service provider is available globally. This is one of the security concerns in cloud computing.

IV. Multi-tenancy

Implementation of multitenancy can be seen when a single resource of application is shared between multiple users. This concept is based on the concept of resource sharing and cost that are associated with these resources among multiple users, thus provides benefits like dynamic provisioning, improvement in usage and efficiency. Thus, cloud use the concept of multitenency to technology for sharing hardware and software resources securely and cost-efficiently between multiple users of cloud.

V. Application Security Issue

The services that are provided by SAAS can be obtained via the web browser over the internet. There arises vulnerabilities in SaaS services due to errors. Since the attackers are manipulating the data through the internet by making data theft. Thus SaaS has different security issues than other services that are provided through web.

III Literature Survey

In [1] authors used cryptographic algorithms to secure data in cloud computing. The proposed system provides security to the files that are transmitted through the network. The combination of RSA and DES algorithm is used to generate the cipher text of the file that is uploaded in cloud storage. On the receiver side the inverse of RSA and DES is performed for decryption of the data in file. First step that us performed is apply DES algorithm on the input file and then apply RSA on the output cipher of the file after applying DES to complete the second encryption level. Thus the cipher is stored in the database. For decryption inverse of the encryption is done.

In [2] author used for secure data communication the cryptography based on DNA message encoding. The Primary Cipher text is generated by using the encryption algorithm which makes use of OTP (one-time-pad) generation scheme of key. Two phases in this technique used are: generation of primary cipher by making use of substitution method thus followed by generation of final cipher by using DNA based coding.

In [3] author uses DNA Cryptography using symmetric algorithm for secure data transfer. The technique used in this paper presents a new type of symmetric algorithm in the field of DNA cryptography. The keys can be used to obtain encryption and decryption phases of cryptography for the input. To obtain key the secured symmetric key generation process is used in which final encrypted data is obtained from initial cipher using random key generated DNA sequences. The system proposes a new encryption algorithm by making use of random key generation of DNA sequence. Three stages of encryption are used in this algorithm- Encryption of the data, Key Generation is done randomly and Decryption of the data. In the first stage the input data is encrypted which is provided as input to the second stage. In second stage key is generated randomly, that is used for next phase of encryption. In the last stage decryption process of the input data takes place.

In [4] author used is DNA Optimized Play-fair Cipher technique for Cloud Data to get more secured . The paper proposes a model for securing the cloud data using DNA optimized play cipher. Simple substitution ciphers can easily decrypted by some attacker as compared to play-fair. In encryption process, input to the algorithm is plain text and the key. Firstly insert the original text and encrypt the data with the key. Then, obtain the binary text from the encrypted text and convert the

binary text into the DNA text. Then, obtain the amino text from the DNA text. These amino texts are converted into the play-fair cipher. Then finally convert the play-fair cipher into the DNA cipher. On the decryption side, the key should be present which is given at the time of encryption process. Take DNA cipher and use the key for decryption of the cipher. In this paper a study for security issues related to cloud is done and proposed a method for securing the cloud data. Play-fair cipher is optimized by the purposed DNA to remove the problems of the old cipher.

In [5] technique used is DNA techniques to secure cloud. In this paper as we know DNA consists of two strands. For encryption process one of the strands is taken as plain text. Randomly developed "secret key" is appended with it. Thus, the plain text strand is mixed with many other strands to hide the original plain text. In the decryption process, as the "secret key" strands are known. Plain text message strands can be recovered by hybridizing it with complement of "secret key" which is placed on the prepared surface, solid support, or on magnetic beads. This proposed approach can be used in 2D image encryption. This model is used for optimization of security of data in cloud computing.

In [6] study is done on DNA cryptography. In this paper one time pad is used as it is considered as unbreakable technique. Thus the length of the key depends on the plain text which is to be transmitted. For encryption process this randomly generated key is used in reverse order for decryption process. The plain text is firstly converted to ASCII code. Then the ASCII code is converted to binary plain text p. Then this binary plain text is converted into packet DNA cipher text using algorithm. Thus, for decryption the packet is obtained by checking the packet number that is attached with the packet. Thus in this way searching in decryption algorithm gets minimized. Thus upon receiving the packet on the receiver side each packet gets evaluated to find substring that exactly matches the DNA key. Thus the binary plain text is obtained and converted to the ASCII to get the original plain text.

In [7] author started working on to break Data Encryption standard which makes more difficulties and more cost for experiment. In [8] technique used is sticker based on DNA Cryptography with the use of enzymes. The strands of memory and also sticker strands are freezed together. Memory complex stickers are used that are converted to memory strands.

In [9] technique used is Encryption scheme using the PCR. Firstly the message is converted into hexa-decimal code, then this hexadecimal code is converted into binary form. These binary digits are converted to DNA form thus considering it as a template of DNA. The DNA sequence is used to perform PCR. Thus, the sequence of DNA obtained is changed. Thus the original message is totally different from the message obtained after encryption. The reverse order is done to obtain the original message from PCR DNA and then it is converted into binary then finally into plain text. Thus, it becomes difficult for attacker to determine the original message.

In [10] scheme used is Encryption scheme. The message is converted into 4*4 matrix and perform the initial permutation. The key is generated and XOR of input message and key is performed. By transposing the matrix secret key is generated of DNA module and then permutations are performed to obtain cipher text.

IV CONCLUSIONS

DNA cryptography has advantages on both hardware and software applications. As the plain text is converted to cipher text by using only 4 nucleotides this becomes very difficult to determine the plain text for unauthorized user. To provide secure network cloud computing promises a good solution .As security is the measure concern in cloud computing. Thus DNA cryptography can be used with many schemes that can be used in various fields to solve huge problems.

REFERENCES

1. *S. Shakeeba. R.R. Tuteja "Security in Cloud Computing using Cryptographic Algorithms" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 1, 2015.*
2. *J. Snehal, "Secure Data communication and Cryptography based on DNA based Message Encoding", International Journal of Computer Applications (IJCA), Volume 98– No.16, (2014)*
3. *B. Bonny, "Secure Data Transfer through DNA Cryptography using Symmetric Algorithm", International Journal ofComputer Applications (IJCA), Volume 133 – No.2, 2016.*
4. *K. Ashutosh, P. K.Vinay, "DNA Optimized Playfair Cipher to Enhance the Security of Cloud Data", International Journal of Engineering Research & Management Technology (IJERMT), Volume 3, Issue-4,2016.*
5. *A.R. Nimje, "Cryptography In Cloud-Security Using DNA (Genetic) Techniques", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue5, 2012.*
6. *Y.pruthi. S.Dixit "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 4, Issue 5, 2014.*
7. *D. Boneh, "Breaking DES using Molecular computer", American Mathematical Society, pp 3365, 1995.*
8. *Zhihua Chen. "Efficient DNA Sticker Algorithm for DES" pg 15-22.IEEE 2008.*
9. *G. Z. Cui, "New Direction of Data Storage: DNA Molecular Storage Technology," Computer Engineering and Applications, vol. 42, pp. 29–32, 2006.*
10. *Guangzhou Cui "An Encryption scheme using DNA Technology", IEEE pg 37-42 ,2008.*
11. *Tariq H.; Agarwal p.: " Secure Keyword Search using dual Encryption in Cloud Computing" in International Journal of Computational Intelligence Research, Volume 13, pp. 1271-1282 2017.*
12. *Kashyap S.; Madan N. : "A Review on: Network Security and Cryptographic Algorithm", in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, pp. 14141418 (2015)*
13. *Li J.; Wang Q.; Wang C.; Cao N.; Ren K.; Lou J. W. : "Fuzzy keyword search over encrypted data in cloud computing," in the proceedings of IEEE INFOCOM, pp. 1-5,2010.*
14. *Mahajan P.; Sachdeva A. : "A Study of Encryption Algorithms AES, DES, and RSA for Security", in Global Journal of Computer Science and Technology Network, Web & Security, Volume 13, Issue 15, Version 1.0, pp. 15-22 2013.*
15. *D. Jamil and H. Zaki, "Cloud Computing Security," International Journal of Engineering Science and Technology, Vol. 3, No. 4, pp. 3478-3483, (2011).*