DNA Cryptography An New Approach to Secure Cloud Data

Vinay kumar Pant
M.Tech. (CSE)
Subharti Institute of Technology and Engineering Meerut, India
vnpant51@gmail.com

Ashutosh Kumar
Assistant Professor (CSE)
Subharti Institute of Technology and Engineering Meerut, India
ashutoshk8685@gmail.com

ABSTRACT: The advancement of technology rises many of new area of computer technology, cloud computing is one of them. It is a new conceptual based service that use by many small and big organization. In a cloud computing data may be stored at varied locations, both physically and geographically. Cloud computing support the client and server technology. Cloud computing have some important feature like cost effectiveness, easy to use and resource sharing, which proof the importance in the field of computer technology. So user want to use their services to save their cost and expenditures. But one another important things is security of application and services that provided by cloud provider. It is a very big issue for cloud user that which service they are use, how much this is secure. Now a days we are using many algorithms and cryptographic techniques for security of data. Some of them is very powerful and secure but some need to modification. In this paper we purpose a new approach of cryptography that is DNA cryptography. The idea behind to implement DNA cryptography is to enforce the other conventional cryptography techniques and algorithms. Our aim is to build a secure and confidential data over a cloud.

Keywords: cloud computing, data security, DNA, Decryption, Encryption.

I. INDRODUCTION

Cloud computing is a way to move the standalone computer programs and data to virtual server or web for the easier access of users. Cloud computing consider as a next generation technology that revolutionized the IT industry. Cloud computing provides a vast infrastructure to user for performing their tasks and store data. Cloud computing consist two type of model, one is service model (PaaS, SaaS, IaaS) and another is deployment model (Public, Private, Hybrid).The cloud customer does not want to work with single cloud provider due to compatibility issue, service availability issue and sometime insider problem. So they are use multiple cloud services according their demand. In the field of computer science and IT security of application and services are more promising area of research. User of cloud transfer their applications and data to the cloud environment, so it is necessary that the security methods used in the cloud are better than traditional methods. Unauthorized access of data, network and application by an unauthorized person (hacker) are cause lack of security and protection for cloud environment, which effects productivity and growth of the organization [3]. To determine the level of risk durability and concentrate on reducing the risks is the one of the most important part of cloud that cannot be neglected by the cloud service provider. Cloud computing have some important features that overcome the features of traditional services and help in the growth of modern IT industry.

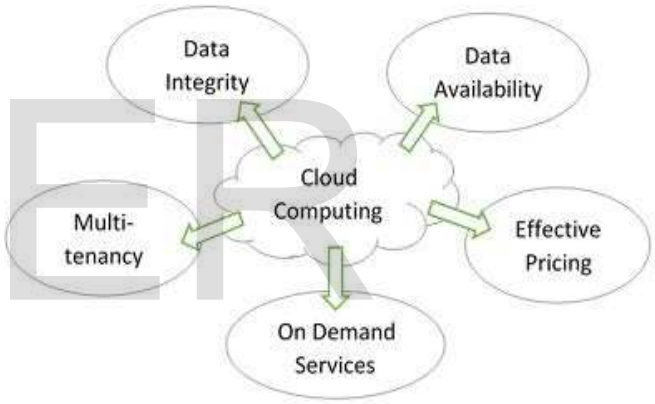

Fig.1. Feature of Cloud

A. *Data Integrity*

Data integrity assure that the information is absolute and valid. Integrity include controlling the network device and data from the unauthorized access or maintain them strictly [3]. It also contains some feature like atomicity, durability, isolation and consistency. Cloud service provider should ensure about data integrity and provide trust to the user for their data privacy or security.

B. *Data Availability [2,3]*

Availability define as all the data and information are continually available at a required level that are requested by customer. So we can say that all machines

have to stored data and application and deliver or process information when the user need them. Cloud venders are use authentic back up system to store and save the customer data, for security of data they use proxy server and according to the users need they deliver data over the network (web). The storage area network (SAN) and network-attached storage (NAS) are two popular approaches to providing data availability.

C. *Multi-tenancy [3]*

It is one of the most important feature of cloud computing. Multi-tenancy define the facility where a single instance use by group of users. Multi-tenancy applies all the three layer of cloud (PaaS, SaaS and IaaS). In cloud this feature provide the service to user to access software applications, databases and hardware resources with specific privilege. Virtualization and remote access give the new meaning of multi-tenancy in the cloud computing.

D. *On-demand Services*

Cloud computing provide the facility for vender to use the applications, software, databases and the hardware resources according to their need and requirement. Cloud user should be able to use computing capabilities when they are needed without the direct interaction with service provider.

E. *Effective Pricing*

Cloud computing provide the cost effective services to customer. A business person who start their new business are need allot of services. If he establish all their own infrastructure for his business so he need invest so much of money. Perhaps this if he take the services of third party provider (cloud provider) they save the money. Cloud services work on the basis of pay per use.

II. CLOUD INFORMATION SECURITY PROBLEMS

Cloud computing face main problems today most popular is confidentiality and integrity of data. Cloud user store their data in multiple storage devices that are provided by cloud venders. But problem is that user doesn't know the location where the data are store and doesn't have the control on that. Some of the security issues are following:

1. *Data Acquisition [3]*

Data acquisition is a method or technique that help to acquire data from different hardware. Cloud user and service provider should know about, how and where are we access the data for that they know the data stream and Peer to Peer operations.

2. *Integrity and Authenticity*

Data integrity means securing data from unauthorized deletion, fabrication or modification. Cloud services work with multiple servers, databases, networks and applications [2]. So managing integrity of data in cloud is very difficult task. Authenticity indicate the process of controlling access of data and information. Only those user access the data that are authorized. Cloud is open source of information so some time many user face the problem of authorization and data access. So these two are big issue with data security in cloud.

3. *Multi-tenancy [3]*

Multi-tenancy define as where cloud systems shared computational resources, Storage, network and services. It is a cost saving and provide better utilization of resources. But harmful for the confidentiality of data due to shared resources. Many malicious activity destroy the servers and network resources so controlling the data or information flow (leakage) are difficult. Virtual machine attack is one of another problem with multi-tenancy.

4. *Attacks*

In modern era of information technology the internet provide a lot of facility to user. Some intelligent computer user use it for illegal activity that increase many security problem, like cyber-attack. Cyber-attackers use malicious code to change computer data that results the harmful effects and user compromise with the data. These activities lead to cybercrimes, such as information and identity theft. Some major attack are Identity theft, malware, phishing, spoofing, Trojans and viruses, password sniffing, Denial-of-service (DOS) and distributed denial-of-service (DDOS) attacks [4]. So we need a powerful method to secure the data.

5. *Application security issue [6]*

SaaS applications are typically delivered via the Internet through a Web browser. However, errors in web applications can create vulnerabilities for the SaaS services. Hackers have using the internet to understanding user's system and perform malicious activities such as steal sensitive data. Security challenges in SaaS applications are not different from any web application technology, but conventional security systems do not effectively protect it from attacks, so we need to new approaches for protection of application.

6. Resource Pooling and Rapid Elasticity issue [6]

Different types of hardware and software resources are integrated for efficient use in cloud environments. This heterogeneity may cause faults as security settings may differ for different kinds of resources. Information leakage is another problem caused by shared resources.

III. Method Used for Security of Data

Security methods and technique used by cloud provider are need to regular updation. Many security thread attack for destroy the data on web or they try to theft the information from the web (cloud). So we need to develop a secure method. Now a days we are use many security algorithms like RSA, ECC, DSA and HASH or some other technique [9]. Some important and vastly used methods are following:-

1. Cryptography [3,10,7]

Cryptography is a method in which we protect data or information and transmit it into an unreadable format. Cryptography play major role to secure ATM transmission, E-commerce, digital media privacy and web data transmission or storage. Modern cryptography work for four major concerns these are non-repudiation, integrity, authentication and confidentiality. In cryptography we use two processes, encryption and decryption.

1.1. Encryption and Decryption [3,10]

Encryption is the process to change information (called plain text) into an unreadable secret format (called cipher text). This cipher text could not be easily understood by somebody except authorized parson. Decryption is the process to converting cipher text back into plaintext. The main motive of encryption is to secure the confidentiality of data stored on computer systems or transmitted via one user to other on network (web). In process of data encryption and decryption the user generate a key and use same or different key to decrypt the cipher text or find plain text (information).

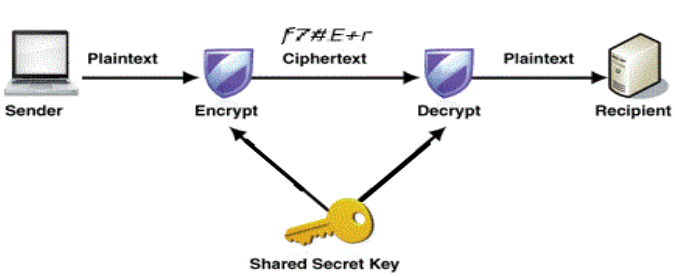

Fig.2. Data Encryption and Decryption Process

2. Steganography

Steganography is the technique or art of hidden writing. In process of steganography we hiding a secret message within an ordinary message (Image, Video and Audio) and the extract message at its destination [10]. We basically study three categories of steganography, secret key steganography, public key steganography and pure steganography. Its advantage over the cryptography is that the earmarked secret message does not attract attention of third party [8]. So storing and sending data on web is very secure using this technique.

IV. Proposed Security Method for Cloud Data

In this paper we purpose a new method of cryptography to secure cloud data, which is a DNA cryptography.

1. Overview of DNA Cryptography

Development of internet services and application promote the security requirement that become more important now a days. We need a complex security machenism that colud not break easily and provide efficient speed of data transmission. DNA cryptography is a new area of cryptography research which drived from the biology. The work on DNA computing started by Adleman and open the new way for the scientist's to do the research in the field of bio-computing [5]. Gehani et al introduce the first algorithm in the field of DNA cryptography. DNA based crytography are used very less amount of system and applications. A simple work in this field were done by Amin et al. He proposed DNA based algorithm (Symmetric Cryptography) called YAEA [12]. So we have a lote off opportunities in the field of DNA cryptography.

2. Biological Background of DNA

DNA (Deoxyribonucleic acid) is a kind of genetic material that help to transfer the information in the living organisms, like small organisms (viruses) to complex one (human) [1]. DNA is a double halix structure that proposed by watson and crick. This DNA structure made by long chain of polymer called nucleotides. Every nucleotide made of three essential component these are nitrogenous base, sugar and phosphate. Basicaly nitrogenous base consist two type of bases pyramidin and puren (Cytosine, Adenine, Guanine and Thymine).

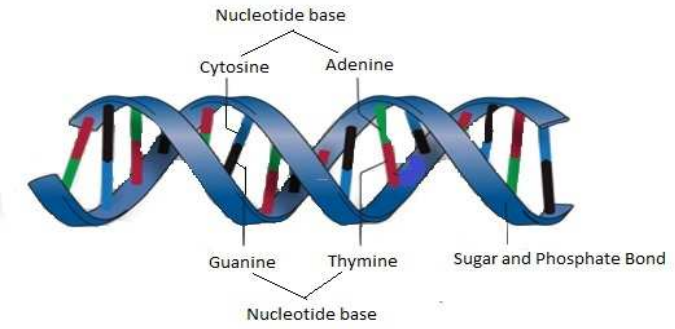

Fig.3. Double Helix Structure of DNA

3. *Related Work*

Advancement of technology and more uses of internet improve the storage capacity of data as standalone storage devices or virtual storage devices. But this advancement also rises some problem basically related to data security. In cloud computing we deal with a hues amount of data that store in remote locations (virtual servers). So security is a more important concern of cloud computing. Here we work with a new idea to secure the data on cloud with the help of DNA cryptography.

3.1. Algorithm for Data Encryption

For the process of data modification we use a symentric key that use for data encryption and decryption both. We follow the following step to encrypt the data.

- Insert the original text 'p'.
- Use the key 'k'.
- Convert the original text into binary text 'b'.
- Now covert binary text into corresponding DNA base pair (amino acid group).
- Now we finally found the DNA cipher 'dc'.

Fig.4. Plain text and key input form

Fig.5. Plain text to binary conversion form

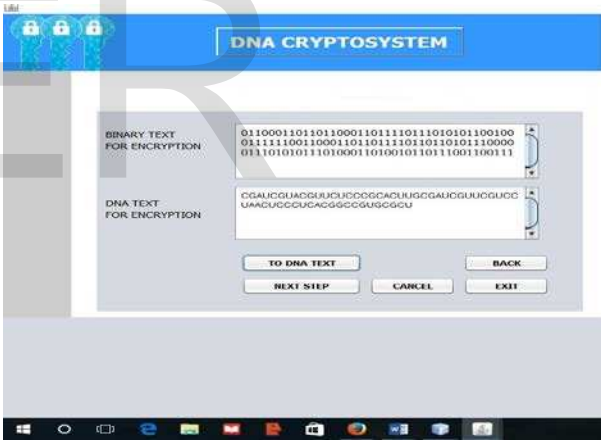

Fig.6. Final DNA encryption form

3.2. Algorithm for Data Decryption

Encrypted data is unreadable for all the user so we need to decrypt the data. In this process we retrive plain text from the cipher text. So we have following step to decript the data.

- Take the cipher text 'dc'.
- Now use key 'k' that provide the time of encryption.
- Convert DNA cipher 'dc' into binary text 'b'.

- Now this binary text converted into original text 'p'.
- Finally we get our original message.

Fig.7. Decryption form

Fig.8. DNA to binary conversion form

Fig.9. Binary to plain text conversion form

Fig.10. Final form to show original text

V. Future Work

Data security is a more promising area of IT industry. The unlimited use of internet and new invention of technology oblige to human being to think about the security of data or internet data. In this paper we discuss a new approach DNA cryptography to secure data in cloud. The very less amount of researches were done in the field of DNA cryptography. I hope this work help to secure data form outsider or hacker, who destroy the important data. In future I want to work to improve the working of this algorithm and also use some other techniques with DNA cryptography that helps to secure the information on computer or internet.

VI. Conclusion

Present time of information technology are fully based on online service or web services. Small organization want to save their money from every time investment on infrastructure development. So they are use online service according their requirement. Cloud computing is a field that provide all the service related to software, infrastructure and storage. This paper discuss feature of cloud, security issues in cloud computing and a new technique of DNA cryptography. This is also discuss how DNA cryptography secure the data. The approach we have use in this paper, will help to make a strong structure for security of data in cloud computing field.

References

[1] Yunpeng Zhang, Xianwei Zhang,"DNA Cryptography Based On Fragment Assembly", Information Science and Digital Content Technology(ICIDT), 2012.

[2] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.

[3] Vinay Kumar Pant, Jyoti Prakash, Amit Asthana, "Three Step Data Security Model for Cloud Computig based on RSA and

Stegnography Techniques", International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.

[4] K.S.Suresh, K.V.Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, 2012.

[5] Xiao Guzhen, LU Mingxin, QIN Lei, LAI Xuejia, "New field of cryptography:DNA cryptography", Chinese Science Bulletin, vol.51 No. 12 1413-1420, 2006.

[6] Vinay Kumar Pant, Mr. Anshuman Saurabh, "Cloud Security Issues, Challenges And Their Optimal Solutions" International Journal of Engineering Research & Management Technology, ISSN: 2348-4039, Volume 2, Issue-3, May- 2015.

[7] M.Kaur, M.Mahajan," Implementing various encryption algorithms to enhance the data security of cloud in cloud computing", VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 10, October 2012.

[8] P.Kalpana, S.Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[9] M.Marwaha, R.Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, P. 367-370, January 2013.

[10] William Stalling, "Cryptography and Network Security-Principles and Practices", Third Edition, publication-Pearson.

[11] E.Gorelik, "Cloud Computing Models", Massachusetts Institute of Technology, January 2013.

[12] Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA based Implementation of YAEA Encryption Algorithm", Internation Conference on Computational Intelliigence, San Francisco, Nov. 20, 2006.