International Journal of Engineering Research & Management Technology ISSN: 2348-4039
July-2016 Volume 3, Issue-4
Email: editor@ijermt.org www.ijermt.org

DNA Optimized Playfair Cipher to Enhance the Security of Cloud Data

Ashutosh Kumar
Assistant Professor (CSE)
Subharti Institute of Technology and Engineering
Meerut

Vinay Kumar Pant
M.Tech (CSE)
Subharti Institute of Technology and Engineering
Meerut

***ABSTRACT*:** *Cloud computing is a modified form of Grid computing and Network Computing. It provides a hues amount of services to user. All the services that provides by cloud computing it's based on internet. It is very flexible, cost-effective way to deliver services to organizations or IT users. Even many feature of cloud computing, the organizations or industries are slow to adopt it, due to the security issues. In cloud all the services provide by third party provider so security issue increases. Users are not aware about many of services that they are use. So the chances of information leakage are increases. For security of data we are using many of technique and security algorithms. Some of these methods are not appropriate for the security of cloud data, they need to modification. In this paper we use DNA optimized Playfair cipher to secure the cloud data.*

KEYWORDS: *Cloud computing, Security, DNA, Playfair.*

1. INTRODUCTION

Cloud computing is a new promising area of information technology. The word 'cloud computing' describe as "A type of internet (web) based computing". Cloud is an Internet based Service provided to the User on their demand. It provide the services like storing, accessing and sharing computer resources over internet, instead of local computers or servers. Customer doesn't need to worry about implementation or maintenance of application and services because all the facilities are provided by the cloud service provider. According to Gartner's study Cloud Computing consider as one of the most important area of the IT industry. Now a days Cloud Computing became the more important part of organizations and scientific communities. Cloud Computing authorize universal, on-demand, appropriate network access to a shared computing resources (e.g., applications, servers, storage, and services) that can be expeditiously provisioned and absolved with minimal management effort or service provider interaction. 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) [5]. The cloud has different architecture based on the services they provide. The data are organized at one centralized place called data centers, keeping a large size of data storage. That data processed using online servers.

Fig. 1. Basic Structure of cloud computing

So, the customers have to trust the vendor on the availability as well as data security. Even if there are so many benefits to opt Cloud Computing, but some limitation stop the way to adopt it by user. The most significant problem with cloud is security, followed by issues regarding integrity, privacy and authentication. According to IDC survey conducted by IT executives and business associates, the top issue in cloud computing is Security. Cloud user 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 [8].
We discuss various security issues for Cloud Computing according modern industries need. We also purposed a security method that help to solved security issue of cloud computing.

2. SECURITY ISSUES WITH CLOUD

Cloud computing provides a number of resources such as servers, storage, networks and some other computing resources that are connected in the form of virtualized systems, they are accessed via the web.

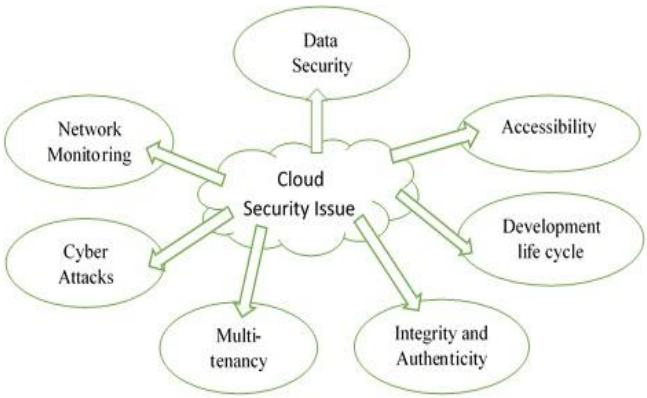

Fig.2. Simple view of Cloud Computing security issue

2.1. Data security issue

Data security is a common issue, but it becomes a major challenge when SaaS users have to rely on their providers for proper security [4]. The SaaS vendor is the one responsible for the security of the data until is being processed and stored [5]. Many cloud service providers provide very few details about their data centers and operations. Hence customer or user does not known about data security.

2.2. Accessibility issue

We access SaaS application anywhere, from any network device easily, including public computers and mobile devices. But most important things is internet connection, without internet we can't be able to access application. So we are fully dependent on web and are no longer access our application offline. Other thing is we use mobile devices that are not fully secure to access application. Some vulnerabilities found in the device OS and official applications that cause of hacking.

2.3. Multi-tenancy issue

Multi-tenancy is one of the major feature of cloud computing. As a result of multi-tenancy, multiple users can store their data in a single instance server using the applications provided by SaaS [6]. This is the approach where we use resources very efficiently but scalability is limited. Since data from multiple bearers is likely to be stored in the same database, the risk of data leakage between these bearers is high. We need to the some security policies that ensure one customer data are hold separate from other customers.

2.4. Development Life Cycle issue

In application development, developers face the complexity of building secure applications that may be hosted in the cloud. At the way where services and data will change or move in the cloud will affect both the System Development Life Cycle (SDLC) and security [8]. Developers have to keep in mind that PaaS applications should be upgraded frequently, so developers have to confirm that their application development

processes are flexible and adequate with changes [6]. The Secure system development life cycle (SSDLC) is new till now and not widely used. Improper use of code and design rise the issue of insecure SSDLC.

2.5. Network monitoring issue

In IaaS model, providers are responsible for network monitoring to sustain acceptable level of QoS. The network monitoring involves a process that keeps track the status of troubleshooting, malicious activity and fault detection. In cloud, Network monitoring is not easy compared with traditional monitoring because cloud is geographically distributed and depends significantly on resources sharing [12].

2.6. Cyber Attacks

Damage caused by the malicious actions of insiders (person) working within an organization that compromises information confidentiality, integrity or availability. Differences may arises due to trust between insider and their organization [1]. The problem related to insider attack (security) in cloud environment occur within either or both the consumer organization and the provider organization.

2.7. Integrity and Authenticity

Cloud computing poses several data protection challenges for cloud consumers and providers. In case of data security we face different risk related to data integrity, data stealing, data location, or data loss. The exposure or prevention of sensitive data is more important, but it also concerns damage or unavailability of data. In some cases, it may be difficult for the cloud consumer to effectively check the data proceeding services of the cloud provider and thus indeed that the data is handled in a secure way [5].

3. METHODS USE FOR SECURITY OF CLOUD DATA

In modern area of computer science we are use many different technology. So security of data is more important on these technologies. Cloud computing security architecture is powerful only when we use specific method or policy to according their architecture. For each malware and threat, we identify which cloud service model or models are affected by these security problems [10]. There is some simple way or method, which help to secure cloud.

- Identity and access management guidance.
- Digital signature is a technique use to validate authentication and integrity of data and software.
- We also use encryption technique to secure sensitive data. Software developers need to develop good application who provides encrypted data for the security. We have some well-known encryption techniques such as Advanced Encryption Standard (AES). Also, SSL technology can be used to protect data on cloud.
- SLA (Service Level Agreements) is the most important part of cloud services security.
- Recovery of data is one of the facilities which help to protect user data or recovery of information for certain failure of system and network.

4. PROPOSED SECURITY METHOD FOR CLOUD DATA

This paper describes DNA optimized Playfair cipher to secure cloud data. These techniques help to overcome the disadvantage of old Playfair algorithm. We combined the two cryptographic techniques to provide high level of security.

4.1. Playfair cipher

Playfair cipher also pronouns as Wheatstone cipher or Playfair square. It is a first digram substitution cipher, which firstly developed by Charles Wheatstone in 1854 [14]. But use of Playfair cipher promoted by Lord Playfair. The Playfair is difficult to break rather than simple substitution ciphers. It is seen that the rules of encryption applies a pair of plaintext characters. So, it needs always even number of characters in plaintext message. Playfair ciphers neglect the value of low frequency alphabets basically 'I' or 'J'. This problem solved by our purposed method.

4.2. DNA Cryptography

DNA cryptography is the new field of security algorithm. DNA pronounced as 'deoxyribonucleic acid'. The work on DNA computing started by Adelman and open the new way for the scientist's to do the

research in the field of bio-computing [1]. Gehani et al introduce the first algorithm in the field of DNA cryptography. DNA based cryptography are used very less amount of system and applications. Simple works in this field were done by Amin et al. He proposed DNA based algorithm (Symmetric Cryptography) called YAEA [3]. This DNA structure made by long chain of polymer called nucleotides. Every nucleotide made of three essential components these are nitrogenous base, sugar and phosphate. Basicaly nitrogenous base consist two type of bases pyramid in and puren (Cytosine (C), Adenine (A), Guanine (G) and Thymine (T)).

4.3. *Related Work*

In older algorithm had some drawback like unable to encrypt any special characters and every letter was necessary to be in the form of English alphabet. In our purposed method plain text directly convert into binary text (0, 1), so it accepts all the type of input. After that these binary value convert into their corresponding DNA value. The related table to represent the value of DNA is following:

Bit	Bit	DNA
0	0	A
0	1	C
1	0	G
1	1	U

Fig.3. Table for bit representation of DNA Value

4.3.1. *Encryption and Decryption*

Encryption is the process to convert plaintext to cipher text (unreadable form) and decryption is the reverse process which helps to convert cipher text to main text (original message). Here we show how our purposed method worked by the help of block diagram.

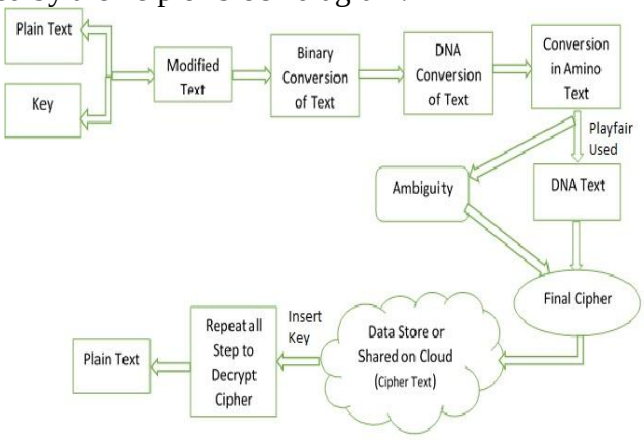

Fig.4. Block diagram for encryption/decryption process

➢ ***Algorithm for data encryption***

For this process we use a key with the input time of plain text. The main steps of algorithm are as following:

- Insert the original text first ‘p’.
- Give the key to encrypt the data ‘k’.
- Convert the text into binary text.
- Now binary text converts into DNA text.
- Convert DNA text into amino text.
- These amino texts convert into Playfair cipher.
- Playfair ciphers again convert into final DNA cipher ‘dc’.

Practical implementations of algorithm are as following:

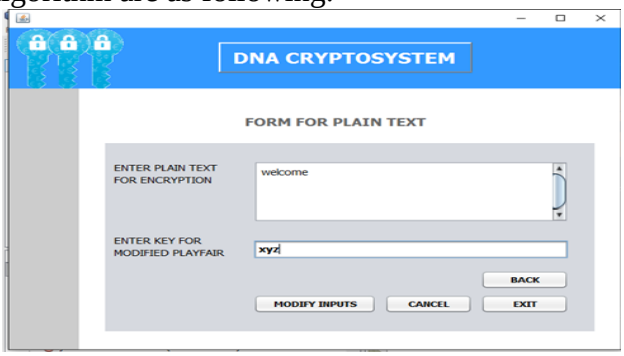

Fig.5. Form for Plain text & key

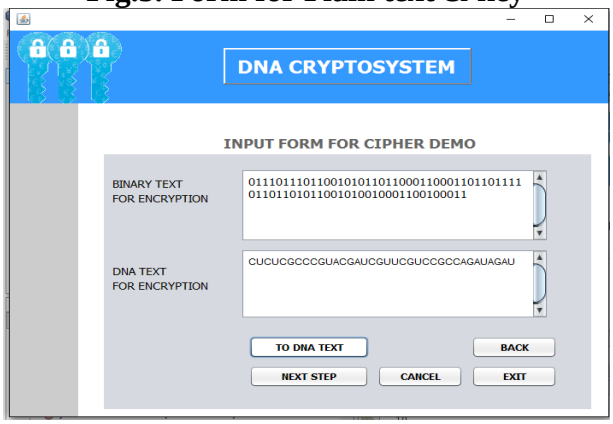

Fig.6. Binary to DNA conversion

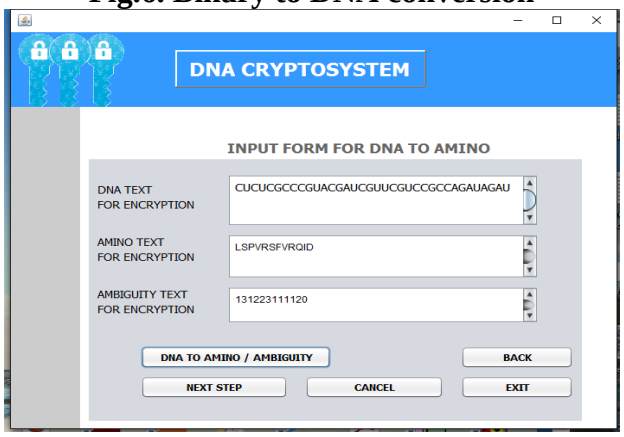

Fig.7. DNA to Amino text

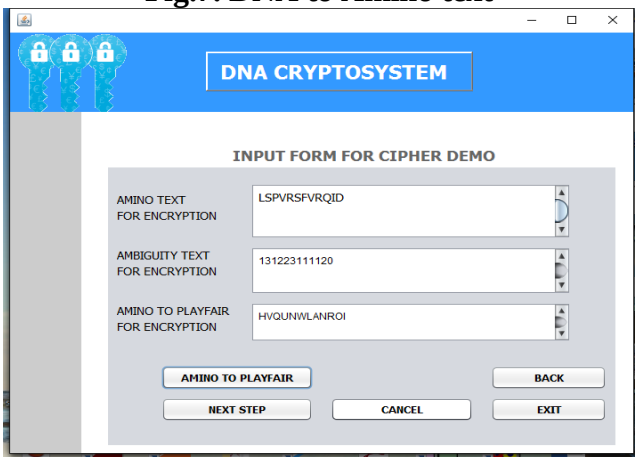

Fig.8. Amino text to playfair conversion

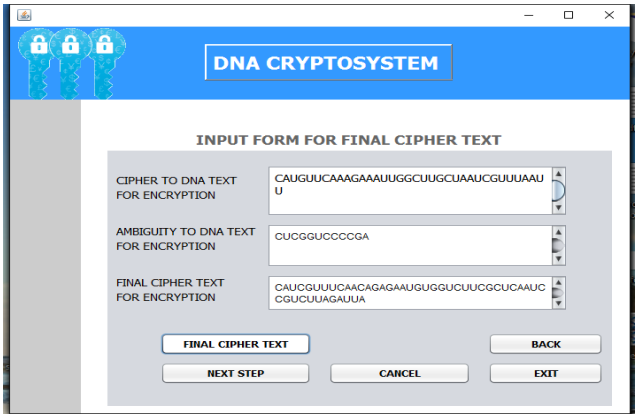

Fig.9. Final cipher text

➢ ***Algorithm for data decryption***

For the decryption process we need key which we given in the time of encryption process. Step of algorithm as following:

- Take DNA cipher ‘dc’.
- Insert key ‘k’ for decrypt the cipher.
- Decrypt from DNA to Playfair cipher.
- Now convert Playfair cipher into amino text.
- Again amino text to plain DNA text.
- Decrypt DNA text into Binary text.
- Now get original text (message) ‘p’.

Fig.10. Decryption Form

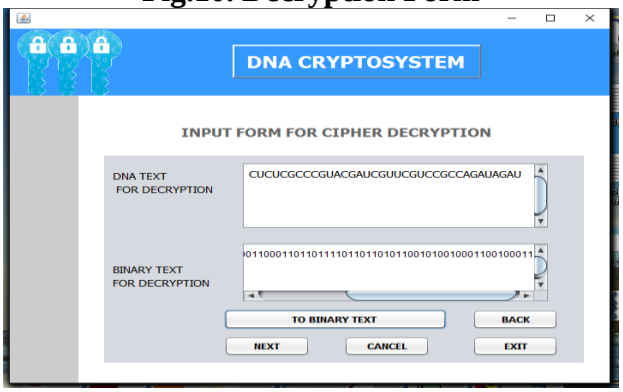

Fig.11. DNA to Binary decryption

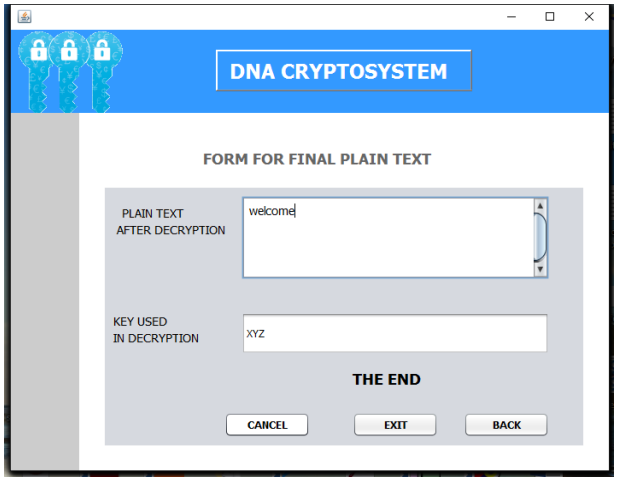

Fig.12. Form for original text

5. FUTURE WORK

Cloud computing revolutionized the IT industries in term of online services. So many organization using cloud service for saving the cost of expenditure which they are invest to develop. Hence security of services or data is an important issue. In this paper we purposed a security method that overcome the feature of old security methods and provide a high level of security. Purposed DNA optimized Playfair cipher remove the drawback of old Playfair method. In future we work for comparative study of my algorithm with another existing algorithm or also work for improving the efficiency of algorithm in term of time and key randomness.

6. CONCLUSION

Now a day's cloud Computing become an important part of IT professional's life and also organization. Understanding of security issue in Cloud will help organizations to use cloud services effectively. Here we study security issue with cloud service and purposed a security method that help to secure cloud data. We need some new security techniques and redesigned traditional techniques that can work with cloud architectures. In this paper with two security technique DNA cryptography and Playfair cipher Playfair cipher is easy to use. But it has some limitation that we discuss here and solved with the help of DNA cryptography. DNA cryptography is new area of security of data and application. Here we try to use combination of these to security method for security of cloud data.

REFERENCES

1. Vinay Kumar Pant, Ashutosh Kumar, "DNA Cryptography An New Approach to Secure Cloud Data", International Journal of Scientific & Engineering Research, ISSN: 2229-5518, Vol. 7, Issue- 6, June 2016.
2. Yunpeng Zhang, Xianwei Zhang,"DNA Cryptography Based On Fragment Assembly", Information Science and Digital Content Technology(ICIDT), 2012.
3. 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.
4. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.
5. 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.
6. 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.
7. Xiao Guzhen, LU Mingxin, QIN Lei, LAI Xuejia, "New field of cryptography:DNA cryptography", Chinese Science Bulletin, vol.51 No. 12 1413-1420, 2006.
8. 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.
9. 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.

10. 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.
11. 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.
12. William Stalling, "Cryptography and Network Security-Principles and Practices", Third Edition, publication-Pearson.
13. E.Gorelik, "Cloud Computing Models", Massachusetts Institute of Technology, January 2013.
14. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam, "A Modified Version of Playfair Cipher Using 7×4 Matrix", International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.
15. Safwat Hamad, Amal Khalifa, Ahmed Elhadad, S. Z. Rida,"A Modied Playfair Cipher for Encrypting Digital Images", J. of Commun. & Comput. Eng., ISSN 2090-6234, Volume 3, Issue 2, 2013.