ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

Cryptography of File with Morse Language and Key Generation Using Zigzag Pattern

Mr.Anand Gandhi[1], Ms.Shradha Allam[2], Ms.Aishwarya Patil[3], Prof. Mrs. A. Nadaph[4]

Student, Comp Dept, KJEI'S Trinity College of Engineering and Research, Pune, India[1,2,3]

Guide, Comp Dept, KJEI'S Trinity College of Engineering and Research, Pune, India[4]

Abstract: Cloud computing offers utility -oriented IT services to users. Cloud computing provides us cheaper, faster, flexible, efficient environment. Cloud computing provides multitudinous benefits to both service provider and customer. A fresh look at the way secure communications is currently being done has been undertaken as a consequence of the large hacking's that have taken place recently.[1]Due to large advancement many companies are migrating to cloud environment. However, the security of cloud computing has been a challenging one. DNA cryptography is used to encrypt message for secure communication on cloud computing environment. Protecting sensitive data is challenging task in cloud environment. For increased security, the recommended approach is to combine two or more methods – processes, DNA cryptography and Morse pattern. DNA cryptography with Morse pattern is difficult to fabricate, which makes the attacker much harder to steal the original data.[2] Use of Morse code and Zigzag pattern makes the attacker much harder to steal original data. Furthermore, the proposed scheme is implemented and the accuracy of encryption and decryption of data is verified.

Keywords: Morse code, DNA sequences, Cloud Computing, Morse Pattern, Zigzag Pattern, Data Block Security, Encryption, Decryption, Key Rotation.

I. INTRODUCTION

The whole world of wireless communications, as we know it today, when Guglielmo Marconi transmitted the Morse code for over a distance of 3 kms by electromagnetic waves. From this time, wireless communications have grown up into a key element of modern society. Electronics devices can exchange information over network by using Wifi. In cloud computing services are ballooning and its multifarious edge makes all the IT industry to migrate from old service model to new on-demand self service model. Despite its growing popularity and increasing demand, cloud computing faces security challenges. The security issues are handled by combining cryptography with DNA computing. The DNA cryptographic techniques help the cloud user and provider to protect their sensitive information from unknown access. Cloud computing has huge security risks as it deals with sensitive information.

II. LITERATURE SURVEY

Backchannelling Quantum bit (qubit) 'shuffling' [1]
Secure Quantum Morse code (Q–Morse) based communications may assist in additional security by backchannelling (slipstreaming) logic gate swarms relevant to the keys composed of living and non-living sensor and device ecosystem integration is plausible. Furthermore this could assist to drive an inclusive 'Internet of Everything' (IOE). Backchannelling (slipstreaming) quantum cyphers use multiple properties that could be unique to the entities. Backchannelling (slipstreaming) the Block chain data as a verification key(s) is plausible if quantum qubit shuffling (containment wave) scaffolding signals has digital states of 'Quantum Morse' (Q–Morse) code. The entangled states.

"Securing Cloud Data using DNA and Morse Code: A Triple Encryption Scheme" [2]
Cloud computing offers utility -oriented IT services to users. Cloud computing provides us cheaper, faster, flexible, efficient environment. Due to various advancements many companies are migrating to cloud environment. At the same time, cloud computing faces more challenges, threats and risks related to data security. DNA cryptography is used to encrypt message for secure communication on cloud computing environment. Protecting sensitive data is challenging task in cloud environment. For increased security, the recommended approach is to combine two or more methods – processes, DNA cryptography and Morse pattern. DNA cryptography with Morse pattern is difficult to fabricate, which makes the attacker much harder to steal the original data. Mentioned DNA based Triple encryption algorithm is more secure algorithm and the correctness of proposed system is checked by using various online encryption tools.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

"Cloud Computing: Technology, Security Issues and Solutions."[3]
This paper has shed some light on the founding technologies of cloud computing such as virtualization and web services/applications. Then the security challenges identified in the literature have been reviewed. These issues majorly circle around two major categories first ones are more traditional issues most importantly the web services and the others are concerned more with the implementation of cloud technology such as virtualization, cloud architecture, cloud deployment models, cloud service models and service level agreements. Further the classification model of security concerns have been provided to help in security issues containment and resolution. This paper also presents the concept and importance of multilevel integrated cloud security in contrast to the famous security-as-a-service concept.

"Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System."[4]

This paper describes an efficient data encryption and data decryption algorithm to protect the outsourced sensitive data in cloud computing environment. With data encryption, data owner can utilize the benefits of file splitting to reduce storage and computational overheads. On the other hand, to reduce the burden of data owner, trusted third party is introduced for verification of authorized users to access the data from cloud server. This demonstrate the performance of encryption and decryption algorithms in terms of data privacy, computational efficiency and effectiveness of the cloud storage system. It also demonstrate for dynamic block level operations on encrypted data blocks for insertion, deletion and update.

"Cloud Computing: A Survey on Security Issues and DNA, ID-base Cryptography."[5]
To overcome the cloud data security challenges, a few recommendations have been proposed along with RSA encryption algorithm. Methods: The RSA algorithm can be defined as an asymmetric key algorithm which is used to develop the strong security model. In cloud computing so many encryption schemes are used for security. In the proposed model the RSA is used to build new security model because it is tightly secured algorithm. Findings: Many organizations are migrating to cloud environment, it is imperative to understand the data security issues surrounding cloud computing. The data security is attained by using modified RSA algorithm. Improvements: In this paper we propose a modified RSA encryption algorithm with longest common sub sequence of a string (LCS). The encrypted and decrypted files are compared and the correctness of proposed system is proved.

III. PROPOSE SYSTEM

In Proposed system we are analysing the information security of authorized user. So, in this paper the User and Admin can register the Application and registration is successful the login the application. So, Admin can upload the file on local disk or cloud. And storage at encrypted format . When File is stored on Cloud or local disk at that time Key are generated and keys .the key are Public ,Private and super keys .Then User see the uploaded file And send the request to the Admin for access on that file. Then admin can send the Morse code key through email to user . Then user can download the file and user can read the file. This file is Decrypted format

IV. SYSTEM ARCHITECTURE

Following diagram is our system's architecture diagram:

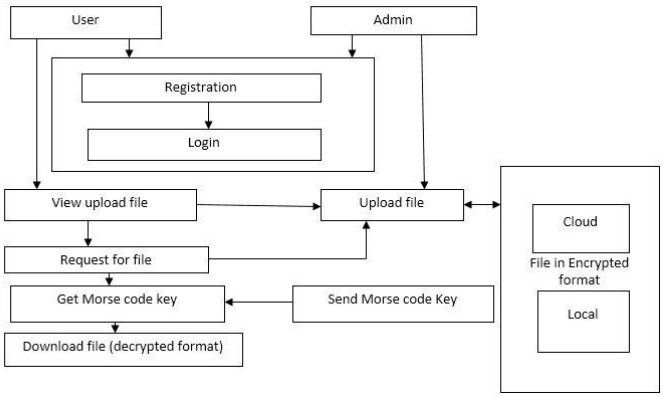

Figure 1: system architecture

In System architecture user and admin login the application. Then admin can upload the file this file can be save in Cloud or decrypted format. Then user can using Morse code key can download the file.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

V. METHODOLOGIES

In that system some Method are used like Key Generation, Decrypted file. Admin can upload the file. Then file is automatically save to the cloud as well as the local system. This file is save as a decrypt format automatically. Key Generation in that when file is save as the cloud or local system. At that time file decrypted format. And Key is generated. This key is three type: -Public Key, Private Key, and Super Key. Then all key is match then it will send to the user and download the file.

VII. APPLICATIONS

High Security in transmitting secret messages at national level.

1. Navy
2. Aviation
3. Military
4. Radio Transmission

VI. CONCLUSION

To improve the security of cloud computing the new model has been proposed. The security model is based on DNA sequences. So finding original data is harder with the existing encryption model and now the Zigzag pattern is added to improve security. Transmitting and storing file over the cloud securely using encryption Decryption over file and Morse code language

REFERRENCES

[1] Backchannelling Quantum bit (qubit) 'shuffling' Quantum bit (qubit) 'shuffling' as added security by slipstreaming Q–Morse Dr John Ronczka. 2016 3rd Asia-Pacific World Congress on Computer Science and Engineering.

[2] "Securing Cloud Data using Dna and Morse Code: A Triple Encryption Scheme" A. Murugana and R. Thilagavathyb International Journal of Control Theory and Applications ISSN : 0974–5572 © International Science Press Volume 10 • Number 23 • 2017

[3] "cloud Computing: Technology, Security Issues and Solutions." Naim Ahmad 978-1-5090-5814 3/17/$31.00 ©2017 IEEE

[4]L. Adleman, "Molecular computation of solutions to combinational problems".American Association for the Advancement of Science, pp.1021-1024, 1994.

[5] Rachna.A, and Anshu.P, "Maintaining Data Confidentiality and Security over Cloud: An Overview", International Journal of Engineering Research and Applications (IJERA), Vol. (4), pp.1922-1926, July 2013.

[6] D.Sureshraj and Dr.V.Murali Bhaskaran, Automatic DNA Sequence Generation for Secured Effective Multi-Cloud Storage, Journal of Computer Engineering (IOSR-JCE), vol.15, pp. 86-94, Nov-Dec 2013.

[7] W.Lizhe, Jie Tao, M.Kunze, A.C. Castellanos, D.Kramer, and W.Karl,"Scientific Cloud Computing: Early Definition and Experience," In HPCC, vol. 8, pp. 825-830. Sep 2008.

[8] P.K.Paul and M.K.Ghose, "Cloud computing: possibilities, challenges and opportunities with special reference to its emerging need in the academic and working area of Information Science," In Procedia Engineering, vol. (23), pp.2222-2227, Jan 2012.

[9] Kandukuri, Balachandra Reddy, and Atanu Rakshit, "Cloud security issues," InServices Computing, 2009. SCC'09. IEEE International Conference on IEEE, pp. 517-520, Sep 2009.