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

Morse Code Security

Gaurav Gawade[1], Gulam M.Khan[2], Indrajeet Gurav[3], Lonkar Kiran Rajendra [4], Prof. Mrs. Vanita Gadekar[5]

Student, Computer Department, Trinity Academy of Engineering College, Pune, India[1,2,3,4]

Guide, Computer Department, Trinity Academy of Engineering College, Pune, India[5]

Abstract: Morse code key is the earliest method used in Radio Telegraphy. To increase security and confidentiality of data in cloud environment, the DNA sequences are used with Morse code and zigzag pattern, for encoding scheme. Use of Morse code and Zigzag pattern makes the intruder 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, Encryption, Decryption

I. INTRODUCTION

The whole world of wireless communications, as we know it today, started in 1895, when Guglielmo Marconi transmitted the Morse code for letter "S"(three-dots) over a distance of 3 kms by electromagnetic waves. From this time, wireless communications have grown up into a key element of modern society. It is the main technology for wireless connection to computer networks. 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

Cloud Computing: Technology, Security Issues and Solutions .[1]
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.[2]
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.

Back channelling Quantum bit (qubit) 'shuffling' .[3]
Secure Quantum Morse code (Q–Morse) based communications may assist in additional security by back channelling (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). Back channelling (slipstreaming) quantum cyphers use multiple properties that could be unique to the entities. Back channelling (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.

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

III. PROPOSE SYSTEM

In Proposed system we are analysing the information security of authorized user. So, in this paper the User can register the Application and registration is successful the login the application. Similarly Admin can Register the application and registration is successful then login the application. Admin can upload the file. So, this file is save to Cloud or Local storage at encrypted format .and keys are generated .the key are Public ,Private and super keys .Then User view the uploaded file And send the request to the Admin for access this file. Then admin can send the Morse code key by email to user and user get the keys. Then user can download file. File is decrypted format.

IV. SYSTEM ARCHITECTURE

Following diagram is our system's architecture diagram:

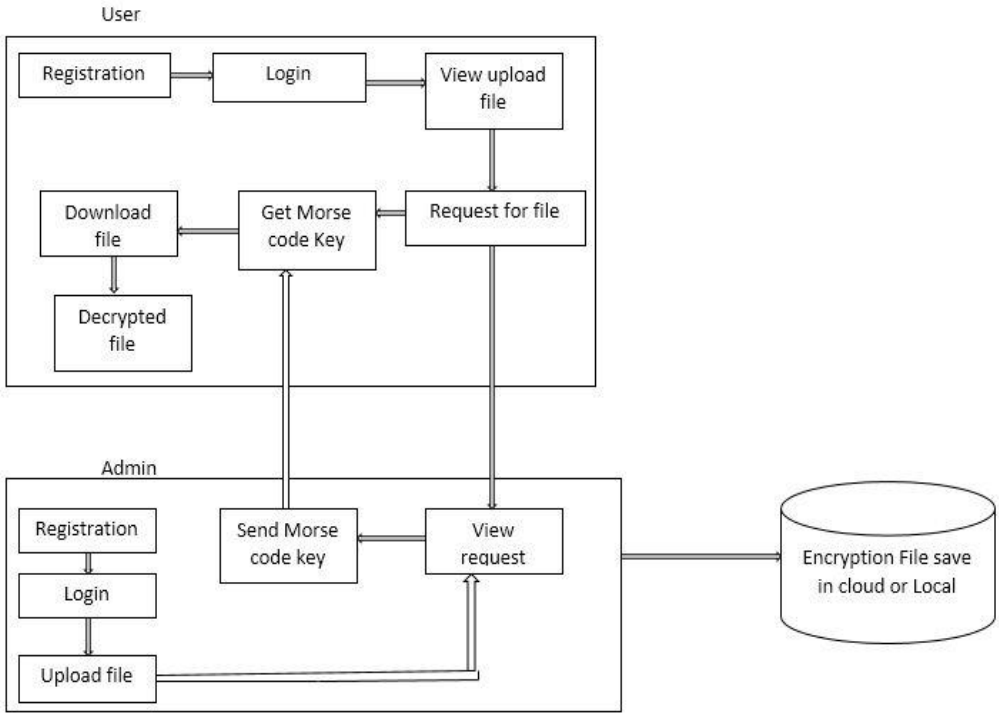

Figure 1: system architecture

In System architecture Admin and user can register the application and registration is successful then login the application. Then admin can upload the file the user can using Morse code key can download the file.

V. METHODOLOGIES

In that system some Method are used like Decrypted file, Key Generation. 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, Super Key. Then all key is match then it will send to the user. Download the file.

VI. APPLICATION

High Security in transmitting secret messages at national level.

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

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

CONCLUSION

Transmitting and storing file over the cloud securely using encryption Decryption over file and Morse code language.

REFERENCES

[1]. Cloud Computing: Technology, Security Issues and Solutions.
[2]. Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System.
[3]. Backchannelling Quantum bit (qubit) 'shuffling'
[4]. 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.
[5]. 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.
[6]. Kandukuri, Balachandra Reddy, and Atanu Rakshit, "Cloud security issues," InServices Computing, 2009. SCC'09. IEEE International Conference on IEEE, pp. 517-520, Sep 2009.
[7]. L. Adleman, "Molecular computation of solutions to combinational problems".American Association for the Advancement of Science, pp.1021-1024, 1994.
[8]. 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.
[9]. 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.