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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

"Survey on Morse Code for High Level Security for Cloud Storage"

Hemant Shinde[1], Rutuja Kadam[2], Gayatri Narayankar[3], Shradha Kokil[4]

Assistant Professor, Department of Computer Engineering, Keystone School of Engg. College,

Savitribai Phule Pune University, India[1]

UG Student, Department of Computer Engineering, Keystone School of Engg. College,

Savitribai Phule Pune University, India[2,3,4]

Abstract: Cloud computing offers the IT services to users. Cloud computing provides us cheaper, faster, flexible, efficient environment. Cloud computing provides multitudinous benefits to both service provider and customer. Security, being the major issues which hinder the growth of cloud computing service model due to the provision of handling confidential data by the third party is risky such that the consumers need to be more attentive in understanding the risks of data breaches in this new environment. Due to various advancements many companies are migrating to cloud environment. However, the security of cloud computing has been a challenging one. For increased security, the recommended approach is to combine two or more methods processes, the DNA sequences are used with Morse code and zigzag pattern, for encoding scheme. 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

Humans are by nature social beings, and that capability has been developed thanks to the verbal and non-verbal communications, through which feelings, thoughts and needs are expressed, as well as, problems are solved. For humans, therefore, expressing their preferences, opinions and feelings is part of their daily life and makes them easier to satisfy their basic needs.[1] 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. WiFi - Wireless LAN. Electronics devices can exchange information over network by using Wi-Fi. 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. The Morse code is transmitted the message in the form of 'dot' and 'dash' 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. To make data more secure from attacks before transmission, the data is encrypted using DNA sequences and stored in the cloud. Cloud computing has huge security risks as it deals with sensitive information.

II. LITERATURE SURVEY

"Backchannelling Quantum bit (qubit) shuffling"[1] Dr.John Ronczka

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.
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.

DOI 10.17148/IJARCCE.2018.71214

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.

“Cloud Computing: Technology, Security Issues and Solutions.”[2]
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.”[3]

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.

III. PROPOSED 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. When File is stored on Cloud or local disk at that time.

This paper describes an efficient data encryption and data decryption algorithm to protect the outsourced sensitive data Rotations for Data Security in Cloud System” Key are generated and keys ..Then User see the uploaded file. Prakash G L, Dr.Manish Prateek, Dr.Inder Singh And send the request to the Admin for access on that file. Then 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.

Author Name	**Title**	**Year**	**Description**
Dr.John Ronczka	Back Channell ing Quantum bit (qubit) shuffing	2016	Backchannelling (slipstreaming)quantum cypher use multiple properties that could be unique to the entities.
Naim Ahmad	Cloud Computi ng: Technol ogy, Security Issues and Solutions	2017	This paper has shed some light on the founding technologies of cloud computing such as visualization and web services/ applications.
Prakash G L, Dr. Manish Prateek	Data Encrypti on and Decrypti on Algorith	2014	This paper describes an efficient data encryption and data decryption algorithm to protect the outsourced

IV. SYSTEM ARCHITECTURE

Following diagram is our system's architecture diagram:

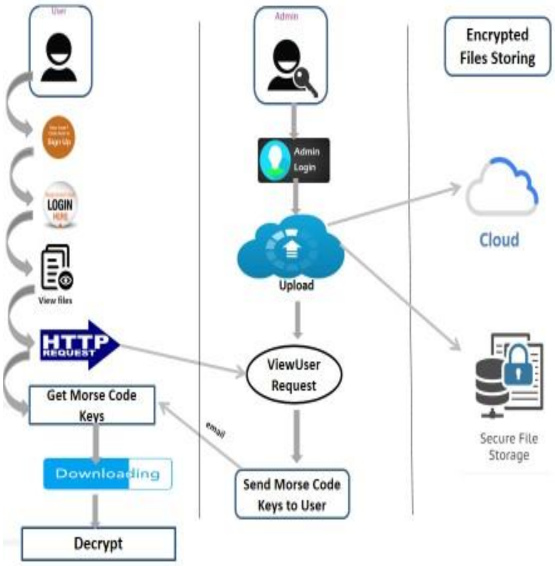

Figure 1: system architecture

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

V. ENCRYPT AND DECRYPT STRINGS TO DNA SEQUENCES

Description

The module is naive and. It transforms text strings into DNA sequences. A DNA sequence is composed of four nucleotides which are represented as A, T, C, G. If we transform "abcdefghijklmnopqistuvwxyzABCDEFGHIJKLMNOPQISTUVWXYZ", the corresponding sequence would be:

TAGACCTGTCGGTGGGTGGTTCCCCGTATGAAGGGGG GGCTATGAGTCTACAGACTGACAGGGGGAGTC AGCGAGTTAGCTAGTAAGCAAGTCCGCCCGTGCGCGC GTTCGCTCGTACGCACGTCGTCCGTTGCGCGGT CGGTCTGTTAGTCAGTTCTTCCTTTGTTCGACGTACAG ACGTACATACGAACAAACGCCCACCCGGCCAG CCGTCCATCCGACCAACCGCGGCCGGTGCCAGGGCGG CTGGTAGGCAGGTCTGCCTGTGTGCGGGGTGG GGCCCACGCCGCACAGCAGCAGGGGGGGGGGGGGC

The transformation is not unique due to a random mapping, but all the transformed sequences can be decrypted correctly to the origin string.

ALGORITHM

First, text file are compressed into gzip files when encrypting and DNA sequences are first decrypted into gzip files and then uncompressed into normal text file. The algorithm behind the module is simple. Two binary bits are used to represent a nucleotide such as '00' for A, '01' for C. If you have some knowledge of molecular biology, you would know that A only matches to T and C only matches to G. So if '00' is chosen to be A, then '11' should be used to represent 'T'. In the module, the correspondence between binary bits and nucleotides are applied randomly. The information of the correspondence dictionary is also stored in the final sequence.

Here is the procedure for encryption:

1. Split a string into a set of letters or characters.

DOI 10.17148/IJARCCE.2018.71214

2. For each letter, convert to its binary form and transform to ATCG every two bits using a randomly generated dictionary.
3. Join the A, T, G, C as a single sequence.
4. Find the first nucleotide of the sequence.

Find the number of the first nucleotide in the sequence. There is a database storing all arrangements of '00', '11', '01', '10'.

Calculate the index value from the number of the first nucleotide by mod calculation. Retrieve the arrangement with the index value, map them to the dictionary and get four nucleotides. E.g. the first nucleotide of the sequence is G. The number of G in the sequence is 40. The number of all arrangement in the database is 24. Then we calculate the index value by 40 % 24 = 16. Then the 16th arrangement is retrieved and may looks like ['01', '11', '10', '00']. The four items in the array are mapped to the dictionary to be four nucleotides such as CTGA. Note this information can be used in the decryption procedure. Put the first two nucleotides at the beginning of the sequence and the last two nucleotides at the end of the sequence. 10. That is the final sequence.

Here is the procedure for decryption:
Extract the first two and the last two nucleotides form the sequence. E.g. CT and GA.
Count the number of the first nucleotide in the real sequence, e.g., 40 for G.
Use this number to calculate the index in the arrangement database, e.g., 16. find the dictionary, i.e. a dictionary is generated from the 16th arrangement ['01', '11', '10', '00'] and CTGA. Translate the DNA sequence according the dictionary into binary bit form and finally to the original format.

VI. METHODOLOGIES

In that system some Method are used like Key Generation and 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, Super Key. Then all key is match then it will send to the user and download the file. And this file is Encrypted format.

VII. APPLICATION

High Security in transmitting secret messages at national level.

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

VIII. ADVANTAGES

1. Unauthorized user cannot be access the file.
2. Data should be secure.
3. Use of the Morse code is a low cost way to send information is to long distances.
4. Communication is secure.

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.

DOI 10.17148/IJARCCE.2018.71214

BIOGRAPHIES

Prof.Hemant Shinde
Qualification: M.EComputer,
Experience: 10 Years of Teaching Experience.
He is expertise in field of Software Development and System Programming.

Rutuja Kadam
Qualification: Currently pursing BE in the Keystone School of engineering.
Her research interests include Database, Programming Languages (i.e C,C++,java) Operating System and Data Structure.

Gayatri Narayankar
Qualification: Currently pursing BE in the Keystone School of Engineering
Her research interests include Database, Programming Languages(i.e C,C++,java,python), Computer network.

Shradha Kokil
Qualification: Currently pursing BE in the Keystone School of Engineering. Her research interests include Database, Programming Languages (i.e C,C++,Python),Testing

DOI 10.17148/IJARCCE.2018.71214