Morse Code for High Level Security for Cloud Storage

Hemant Shinde[1] Rutuja Kadam[2] Gayatri Narayankar[3] Shradha Kokil[4]
[1]Assistant Professor [2,3,4]UG Student
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Keystone School of Engg. College, Savitribai Phule Pune University, India

Abstract— Morse code is designed to be read by humans without a decoding device, making it useful for sending automated digital data in voice channels.[4] 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.[2] 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.[5]

Key words: DNA Sequences, Morse Pattern, Zigzag Pattern, Data Block Security, Key Generation

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.[2] 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. DNA sequence ATGC is the basic sequence of DNA cryptographic technique. The randomness of DNA sequence used to achieve strong encryption algorithms. [4]The DNA computing is high in cost and time consuming. These can be overcome by using modern cryptographic techniques which is based on computer based algorithms. The complex problems can be solved by DNA cryptographic algorithms.

II. LITERATURE SURVEY

Title :Cloud Computing: Technology, Security Issues and Solutions
Author :Naima Ahmad
Description :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.

Title :Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System
Author :Prakash G L, Dr. Manish Pratik, Dr. Indre Singh
Description :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.

Title :Cloud Computing: A Survey on Security Issues and DNA, ID-base Cryptography.
Description: 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.

Title :Morse Code Decoder - Using a PIC Microcontroller
Author :Ms.N.S.Bakde,Prof A. P. Thakare
Description :Morse code is designed to be read by humanswithout a decoding device, making it useful for sending automated digital data in voice channels. For emergency signaling, Morse code can be sent by way of improvised sources that can be easily "keyed" on and off.The design presented here is physically simpler, although the software is considerably more complex.The goal of this project is to produce a system that will decode Morse Code signals from a possibly noisy audio source, and display the decoded text on a LCD screen through a PIC microcontroller interface. The system might also produceMorse code signals via input from a keyboard. It consists of a handheld unit that can receive Morse code, via audio input (internal microphone) or direct signal connection, and translate it for display on an in-built liquid crystal alphanumeric screen.

Title : Cloud Storage Security Scheme using DNAComputing with Morse Code and Zigzag Pattern.

Author :Dr. A.MuruganAssociate Professor, PG & Research. Description : Storing and exchange of data in cloudcomputing become the necessity of modern working pattern in ITindustry. 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.

Name	Title	Year	Description
Naim Ahmad	Cloud Computing: Technology, Security Issues and Solutions	2017	This paper has shed some light on the founding technologies of cloud computing
Prakash G L, Dr. Manish Prateek,	Data Encryption and Decryption Algorith	2014	This paper describes inefficient data encryption and data decryption algorithm.
Dr. A.MuruganAssociate Professor, PG & Research.	Cloud Storage Security Scheme using DNA Computing with Morse Code and Zigzag Pattern	2017	The proposed implemented the accuracy of encryption and decryption of data is verified.
Ms.N.S.Bakde,Prof A. P. Thakare	Morse Code Decoder - Using a PIC Microcontroller	2012	This produce Morsecode signals via input from a keyboard. . It consists PICmicroC between Morsecode input, display unit.

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 & 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 Morse 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

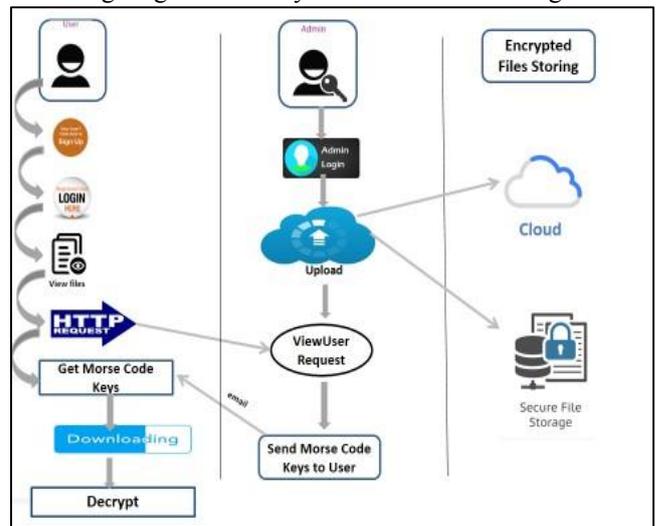Following diagram is our system's architecture diagram:

Fig. 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.

V. ALGORITHM

First, text file are compressed into zip files when encrypting and DNA sequences are first decrypted into zip 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.
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.

A. DNA COMPUTING

DNA computing is a branch of computing which uses DNA and molecular biology hardware, instead of the traditional silicon-based computer technologies. Research and development in this area concerns theory, experiments, and applications of DNA computing. The term "molectronics" has sometimes been used, but this term has already been used for an earlier technology, a then-unsuccessful rival of the first integrated circuits. this term has also been used more generally, for molecular-scale electronic technology.DNA consists of DNA strands which are polymer chains. The polymer chains are composed of four nucleotides. They are, Adenine (A), Thymine (T), Guanine (G), and Cytosine(C).The structure of double stranded DNA with sequence is shown in the following
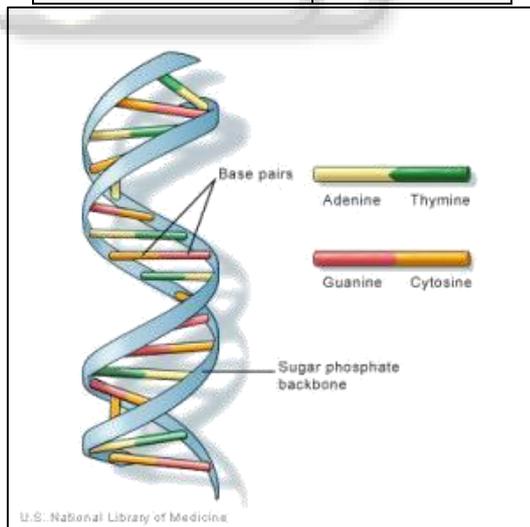
BINARY SEQUENCE		NUCLEOTIDE
0	0	A
1		T
0	1	C
1	0	G

Fig. 2: Double Stranded DNA

B. USES OF MORES CODE

| MORES PATTERN |
|---|
| - . |
| . . |
| . - |
| - - |

As of 2007 commercial radiotelegraph licenses are still being issued in the United States by the Federal Communications Commission. Designed for shipboard and coast station operators, they are awarded to applicants who pass written examinations on advanced radio theory and show 20 WPM code proficiency [this requirement is waived for "old" (20 WPM) Extra Class licensees]. However, since 1999 the use of satellite and very high frequency maritime communications systems (GMDSS) have essentially made them absolute. Radio navigation aids such as VORs and NDBs for aeronautical use broadcast identifying information in the form of Morse Code. Before using such aids, a pilot listens to the Morse code identification to ensure he or she is tuned to the proper aid.

C. ZIGZAG PATTERN

The matrix structure of the N2 integers which would increase sequentially along the arrays anti-diagonally is called Zigzag pattern. The different kind of zigzag patterns is shown in the Fig.1. A motive wave that travels on parallel trend is known as parallel zigzag pattern refer fig.2 (a). The motive wave that travels on parallel trend is known as parallel zigzag pattern refer fig.2. (b). The motive wave that travels on diagonal trend is known as diagonal zigzag pattern refer
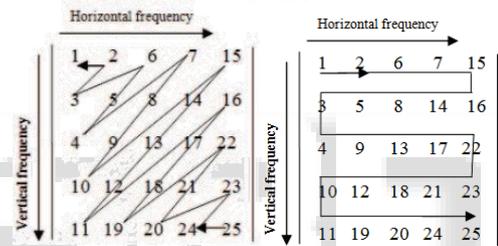
(a).Parallel Pattern.
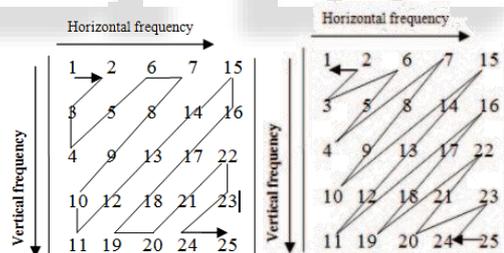
b).Diagonal Pattern.
Fig. 3: Various Zigzag patterns.

VI. MATHEMATICAL MODEL

S= { I, O, Function , success, failure}
Input: Input=filename
Output: Output=Decrypted File
Functions : { f1, f2, f3, f4, f5, f6, f7, f8 }
Where, f1= Admin upload file on cloud
f2= file store on cloud with three Morse code Keys
f3= Duplicate files does not uploaded on cloud
f4= User will see uploaded files on cloud
f5=User request for Morse code key to Admin
f6=Admin give response to user and send three Morse code keys on email
f7= User can download files after entering Morse code keys
f8= User will get file in decrypted form

Success condition = According to proper inputs, three Morse code keys will match for particular file and then file will get download

Failure condition = Wrong inputs, Network Failure, Three Morse key's Mail send or receiving fail, Mismatch Morse code keys.
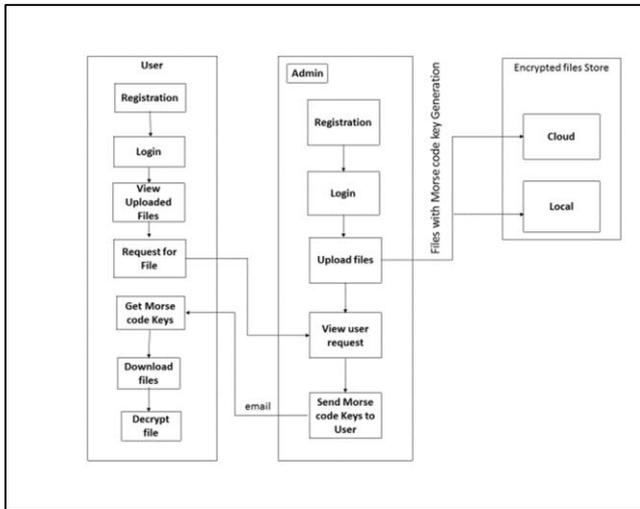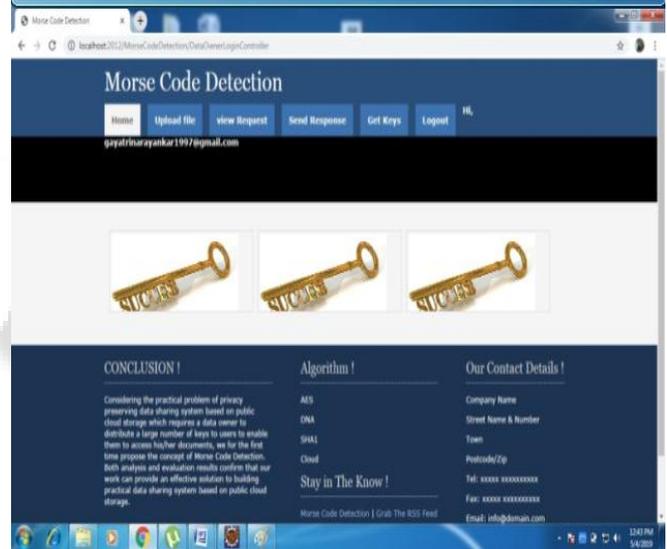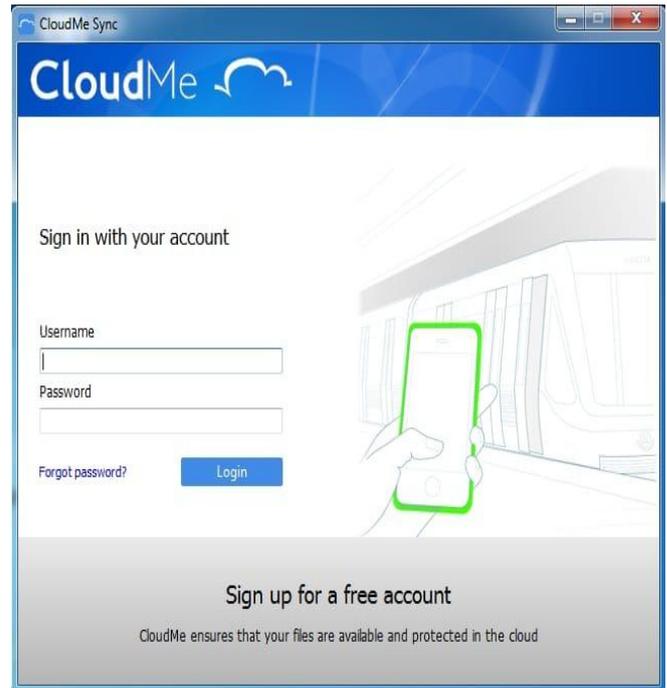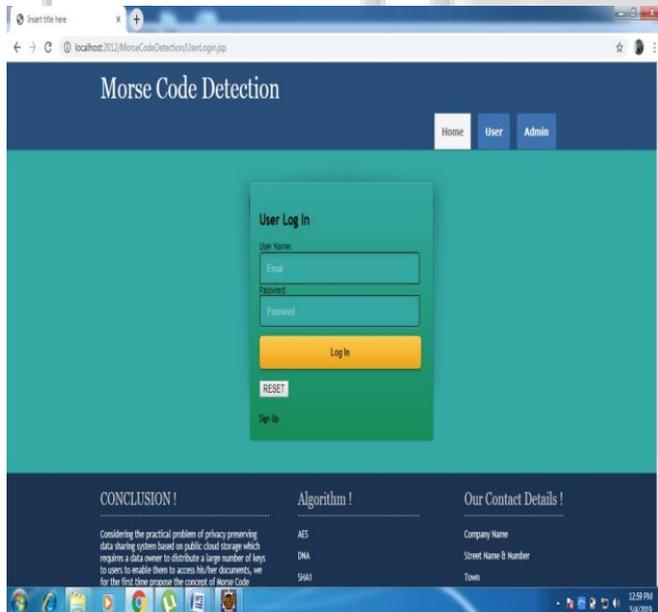
VII. FLOW OF THE SYSTEM

Fig. 4 : Flow of the system

VIII. APPLICATION

1. Military
2. Navy
3. 3.Data Privacy

IX. RESULT

X. FUTURE SCOPE

In future scope we can implement key generation of system using different tech. on cloud and applying different layer of security using cloud storage security storage .

XI. 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.

REFERENCES

[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 Ahmad978-1-5090-5814 3/17/$31.00 ©2017 IEEE

[4] Ms.N.S.Bakde,Prof A. P. Thakare"Morse Code Decoder - Using a PIC Microcontroller."ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR) Volume 1, Issue 5, November 2012.

[5] Cloud Storage Security Scheme using DNAComputing with Morse Code and Zigzag Pattern. *Dr. A.Murugan*Associate Professor, PG & Research. IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017)

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

[7] 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.

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

[9] 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.

[10] 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.

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