ENHANCED CIPHER METHOD FOR CLOUD AUTHENTICATION

Arif Mohammad Abdul[1], Sudarson Jena[2], M Balraju[3], M. Kiran Sastry[4]

[1]*Department of Computer Science, GITAM University, Hyderabad, India*
[2]*Department of Information Technology, GITAM University, Hyderabad, India*
[3]*Department of Computer Science, KITE, Ghatkesar, Hyderabad, India*
[4]*Department of Information Technology, GITAM University, Hyderabad, India*

Abstract

Cloud computing, is a technology that provides dynamic and scalable resources for computing as pay per use through internet. In cloud identifying an appropriate user is a challenging task for the service provider, but basing on the unique identification methods like password, smartcard and many other different authentication techniques, a user can be identified. Even though many authentication schemes are introduced in past but they failed with various drawbacks. This paper is to introduce an authentication scheme using Modified Double ceasar cipher encryption technique in which the password is encrypted using a key that is kept secret and is tough to guess. Our encryption technique is secured from the attacks like guessing or brute force attack. The proposed system uses a Modified Double ceasar cipher encryption technique which uses the English alphabets to create password and a key to encrypt basing on the value of its character by performing addition a cipher key is generated and stored in the waveform. The proposed scheme has an interesting feature of storing and representing the password in waveforms using Manchester encoding [7], which makes the system more effective in avoiding some attacks like guessing attack and tampering the password. The work clearly specifies the different authentication schemes used so far.

Keywords: *Double ceasar cipher, Encryption, Decryption, Authentication, waveform.*

----------***----------

1. INTRODUCTION

Cloud computing is a technology that is introduced based on the very old concept of computing devices using mainframes that uses huge equipments to store and compute large programs in the early days of computers. By modernizing the concept of mainframes the cloud computing is built for providing the space to store the data and many other services for developing their own applications and infrastructure according to the user requirement. It works on the pay per use concept. It has brought a huge change in the way the computing services were traditionally being delivered. This cloud offers platform as a service, software as a service and infrastructures as service, the users are not aware of the location where these services are offered and performed. This model enables the cloud users to increase their usage of data capacity and capability through dynamic access without investing in other infrastructure, licensing new software etc. In cloud computing user authentication is major part in which a correct user is authenticated to access his data. Using password a user can be identified by verifying with unique key at the time of verification. For this we introduce a new concept for password encryption called *Double ceasar cipher*, which is a concept of cryptography using ceasar cipher in which the password encryption is done using a unique key word example “dog” or “king” or any other of fixed length, where as in ceasar cipher only a fixed frequency of alphabet shifting is considered.

1.1 Wave Metrics

The Manchester encoding [7] is the technique for converting the binary data into waveform signals. This helps the data keeping safe and so as the waveform cannot be easily understands by any one. A wave is propagation of any data like audio, plain text etc., into signal that passes through different mediums as follows.

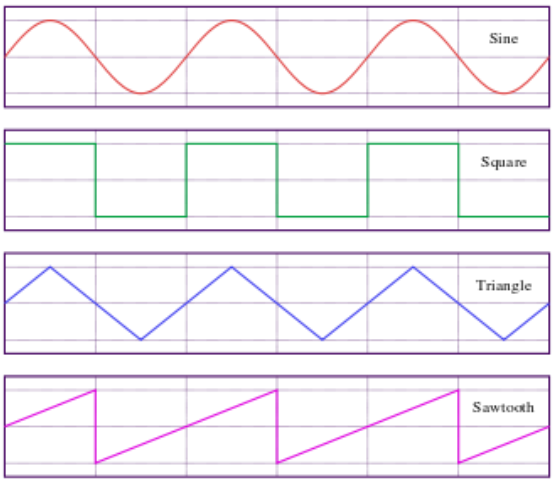

Fig 1 Representing different waveforms

1.2 Manchester Encoding

Manchester encoding technique is a synchronous clock encoding technique used to encode the clock and data of synchronous bit stream.

This technique follows the following rule for encoding.

1. If the original data is 0 - then the Manchester code is 0 to 1(upward).

2. If the original data is 1- then the Manchester code is 1 to 0 (downward).

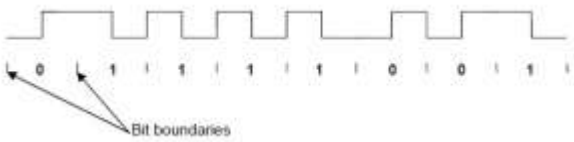

Fig 2 Manchester waveform

The above can be represented as 4 bit-nibbles as follows. If pattern of bits is 0 1 1 1-> encodes to 01 10 10 10.

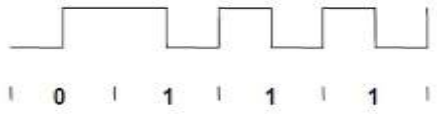

Fig 3 Manchester waveform for 4 bits

1.3 Ceasar Cipher

This is an old way of encryption process, where the English alphabets are considered with a fixed length of shifting for encryption. A plain text is taken for example HELLO YOU and a fixed length of position for shifting say 3 then the shifting is done as follows.
Consider A to Z "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

- The position of the H is shifted left for 3 alphabets that is I -> J -> K. Hence H cipher text is K
- Similarly for all the characters the shifting is done.
- Then the final cipher text is as follows.
- HELLO YOU (plain text) => KHOO BRX (cipher text).

In this technique the frequency key of the shifting can be varied. This technique is very simple and easy to break once if the shift frequency is indentified, as the repeated character will have the same encrypted cipher text that can be easily guessed. For this a modified and enhanced technique is considered to make the ceasar cipher concept strong which is a *Modified Double ceasar cipher,* instead of a fixed shift frequency a key word is considered for encryption, basing on that key word the position of each alphabet is randomly differs and the same cipher text will not be repeated. This technique is explained in detail in the proposed system.

2. LITERATURE REVIEW

Authentication is a process of verifying and identifying the correct user in which the user credentials provided are compared to the values in a database. If the credentials matches, the process is completed and the user is authorized for access. In traditional authentication schemes only a single plain password is used for verification, for which the password is stored in plain text in the user system itself without any password table. This leads to an intruder attack or interception attack. Later using hash functions the password and the user ID is hashed and stored in the form of table at server side, then in the verification phase these values are mapped and verified to get the authentication successful. But here as the password is static with same constant hash values this may lead to modification and man in the middle attack.

To overcome various attacks, in the year 1981 Lamport [1] first proposed a password authentication with insecure communication using smart cards. In this smart card Lamport used Nonce(random number generated at run time), SID(smart card id), PWD(password), Uid(user id). But a drawback in this scheme is that does not maintain verifier table and won't allow password to change freely.

In the year 1995 Gwobao horng [2] proposed a scheme by performing hash functions using XOR operation new values are generated and stored in verifier table. But in this also the table contains the static values for which can be lead to stolen verifier attack.

In the year 2004 Das et al [3] proposed a scheme for dynamic Id based authentication which has a smart card with UID, SID, T(time), Nonce(random number), and x(remote system key) and a dynamic password. For this Mr. Awasthi has proven that in this case if any other person have the fake smartcard or holds some other persons smart card can easily logged in, this shows a very poor authentication.

In the year 2006 Misbah et al [4] proposed a simple and efficient solution. Later after deep study by Sir Misbahuddin in the year 2008 [5] introduced a new technique to overcome the vulnerabilities of Das et al they have introduced a mutual authentication scheme based on time stamps, which is quite difficult to compute the timestamps of client and server system at the same time.

3. EXISTING SYSTEM

The system is based on the authentication scheme using *Passfile* [6]. Which is introduced by Mr. Misbahuddin in the year 2012 from Bangalore university.

- The passfile contains any user defined text, added with two upper case alphabets.
- The text in the passfile in encrypted by hashing and stored as password.
- At the time of verification the content is decrypted basing on the keys like UID, secrete key of remote system, and nonce with SID.
- The passfile is uploaded at the time of registration, which is encrypted and stored.
- Every time the user logins this passfile must be maintained and uploaded for verification.

Disadvantages

- The main drawback of this system is maintaining the passfile.
- Accessing cloud from other remote system is not possible using passfile, because storing and replacing passfile in other systems may leads to malfunction.

- Remembering the passfile name or the text in the passfile is complicated for the user. A small change in the content will make the authentication failure.
- Passfile recovery is tough based on the time stamp for every login.

4. PROPOSED SYSTEM

The proposed system is to introduce a new way of encryption technique using *Modified Double ceasar cipher* on the password which is actually derived from the old cryptography technique Ceasar cipher [8][9]. In the ceasar cipher for every character there is a same cipher value for any number of repeated alphabet, which is a major drawback in the ceasar cipher. The double ceasar cipher process of encryption is done as follows.

- Consider the plain text "HELLO YOU" and a key "KING".
- Now map the characters together.

H	E	L	L	O	Y	O	U
K	I	N	G	K	I	N	G

- Then the position value of the K is taken from the English alphabets and then the number of left shifts is applied on the plain text.
- Suppose values of A-Z is taken as 0-25, then if the value of K= 10, H=7.
- Then apply addition for both values of K in Key and H in plaintext,

  K + H = 10 + 7 = 17.

- Then here considering 17_{th} position alphabet as the cipher text which is R.
- Similarly for all characters of plain text is as follows

H	E	L	L	O	Y	O	U	Plain text
K	I	N	G	K	I	N	G	Key
R	M	Y	R	Y	G	B	A	Cipher text

4.1 Encryption Algorithm

Algorithm Modified double ceasar cipher
1: Input: Plain text = (P1, . . . , PR);
2: Input: Key = (K1, . . . , KR);
3: {Collect user requests (Plainttext and Key).}
4: {Convert (Key and Plain text) into numerical.}
5: {Encrypted text.} Sum
6: for all i <= R do
7: Perform addition for the ASCI values of Plain text and Key alphabets
8: Output: Sum [0-R].
9: The resultant is considered as the cipher text.

4.2 Decryption Algorithm

1: Input: Cipher text=(C1, . . . , CR);
2: Input: Key = (K1, . . . , KR);
3: {Collect (Cipher Text and Key)};
4: {Convert (Key and Cipher Text) into numerical.}
5: {Cipher text} Diff
6: for all i<=R do
7: Perform subtraction for both the cipher text and key;
8: Output: Diff [0-R].

Advantages

- The modified Double ceasar cipher mainly uses a secrete key for encryption, the encryption is done basing on the length and values of the key and plain text.
- Each character has different values at different positions.
- As the frequency of the character changes, guessing the value is not possible.
- For every secret key random cipher text is generated.
- Finding the value of the repeating alphabet is difficult.

5. BLOCK DIAGRAM

5.1 Phase- I: Login or Registration

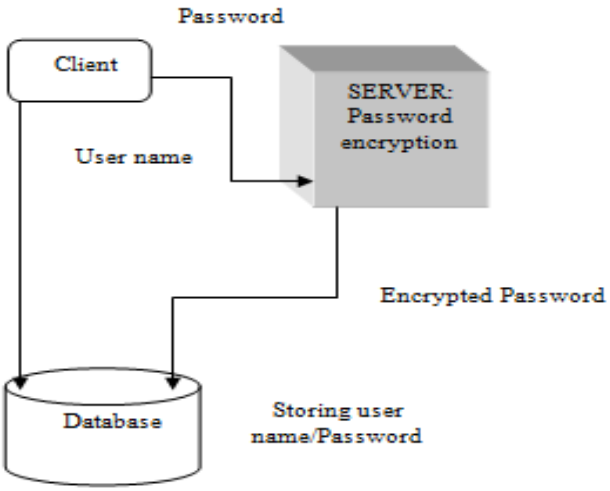

Fig 4 Block diagram for Login/Registration

5.2 Phase- II: Verification/ Authentication

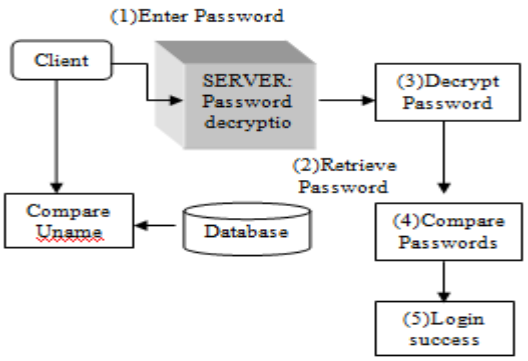

Fig 5 Block diagram for verification

6. RESULTS

Fig 6 Admin Login

Fig 7 User Registration

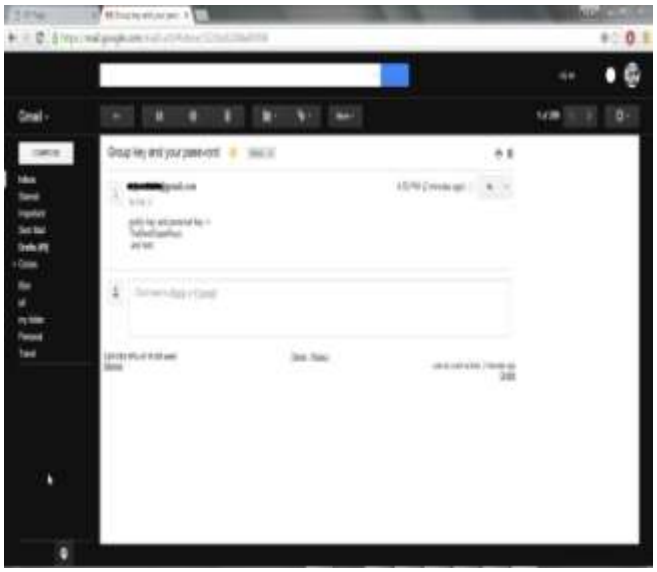

Fig 8 Password Mail after registration

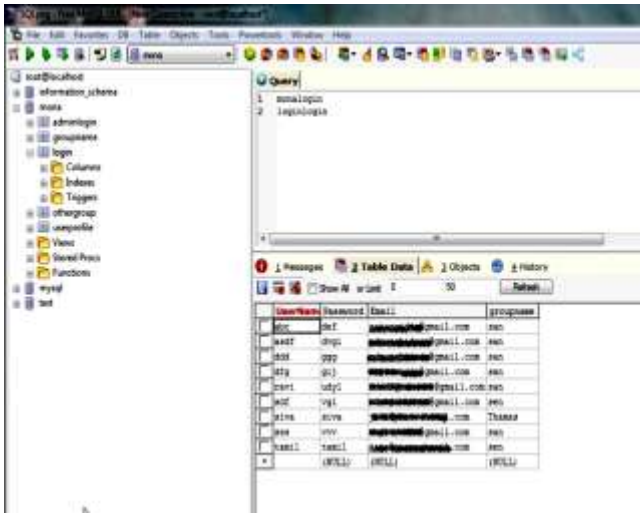

Fig 9 Database before registration

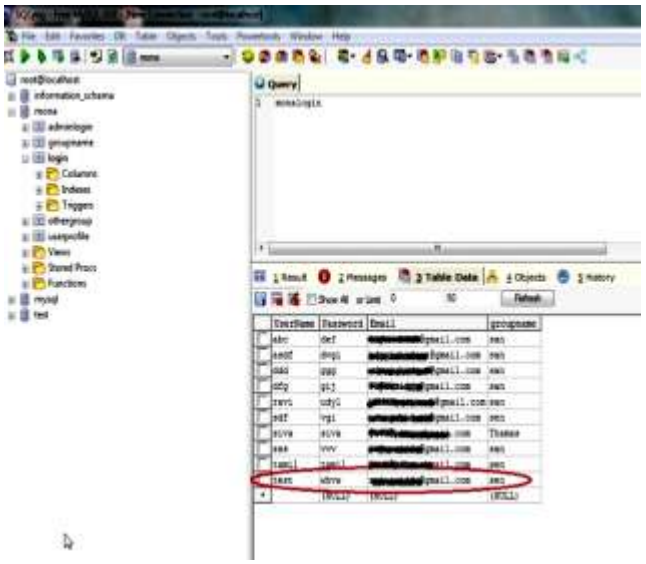

Fig 10 Updated table after registration with ceasar cipher encryption

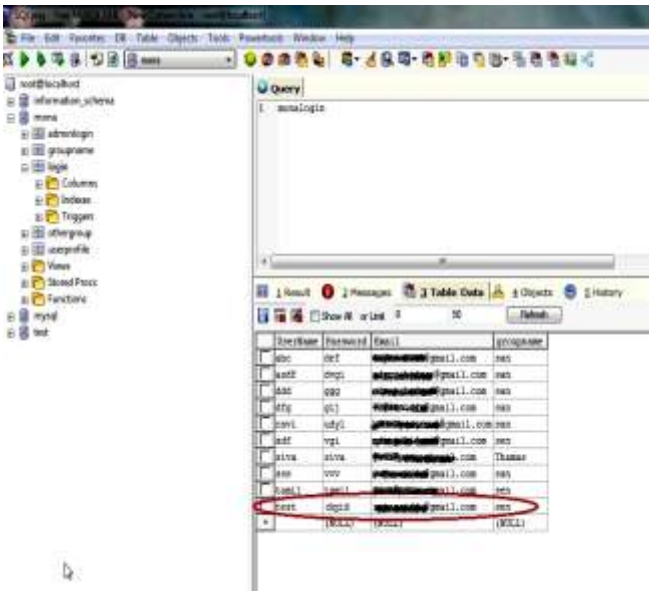

Fig 11 Updated table with modified double ceasar cipher encryption

7. CONCLUSION

Increasing the level of security is the main object using advanced techniques. To provide more security the proposed system presents an implementation of strong authentication system for the cloud environment using an encryption algorithm Modified Double Ceasar Cipher. This authentication scheme uses a plain password for secured login, and is strong in terms of encryption. This scheme is more efficient with random summation of key values with plain text values using ASCI codes and it is secure against brute force attack, guessing attack, and stolen verifier attack. Providing the better authentication schemes for the cloud will enhance the usage of cloud and safe access to any kind of user.

The future work of the proposed scheme is to use the Biometric of any type like finger prints, veins, iris etc, which is interesting and highly secured in authenticating the users. This involves the user himself as a password where only the authorized person will be accessing the cloud by verifying his finger prints or iris or palm veins etc as as password.

REFERENCES

[1] Leslie Lamport, Deparment of computer science, Waterloo university, Canda, 1981. Password Authentication Scheme With Insecure Communication.

[2] Gwobao Horng, Institute of Information Science, National Chung-Hsing University, Taichung, Taiwan, 1995. Password Authentication Scheme Without Using Password Table.

[3] Manik Lal Das, Ashutosh Saxena, Ved P. Gulati, 2004. A Dynamic ID-based Remote User Authentication Scheme.

[4] Mohammed Misbahuddin, Mohammed Aijaz Ahmed, 2006. A Simple and Efficient Solution to Remote User Authentication Using Smart Cards.

[5] Shoba bindu JNTU, Mohammad Misbahuddin Center for development of advanced computers, 2008. Cryptanalysis of Liao-Lee-Hwang's Dynamic ID Scheme.

[6] Syed Akram, Mohammad Misbahuddin, G. Vara prassad, 2012. A Usable Two Factor Authentication Scheme.

[7] Manchester encoding techniques using RS-232, Adrian Mills- Summit Electronnics Ltd 2009, Manchester decoder using CLS and NCO, Jatinder Gharoo, Brain Bailey- Micro chip Technology Inc 2012.

[8] Kashish Goyal, Supriya Kinger, 2013, Modified Ceasar Cipher for Better Security Enhancement.

[9] Enas Ismael Imran, Farah Abdul Ameer, 2014, Enhancement Ceasar Cipher for better security.y