Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 10, October 2013, pg.43 – 47

RESEARCH ARTICLE

SECURED AND RELIABLE DATA TRANSMISSION USING LYCHREL NUMBERS RGB COLORS AND ONE TIME PASSWORD

R. Vanathi[1], L. Dhanam[2], K.R. Senthilnathan[3], M.S. Vinu[4]

[1]Master of Engineering, Department of CSE, Sri Eshwar College of Engineering, Coimbatore, India
[2]Master of Engineering, Department of CSE, Sri Eshwar College of Engineering, Coimbatore, India
[3]Assistant Professor, Sri Eshwar College of Engineering, Coimbatore, India
[4]Assistant Professor, Sri Eshwar College of Engineering, Coimbatore, India

[1] vanathirp@gmail.com; [2] laksh.kavi96@gmail.com; [3] senthilnathanraj@gmail.com; [4] vinuja@gmail.com

Abstract— The main objective of Securing data transmission by xml using lychrel numbers, RGB colors and one time password. The universal technique for providing Cryptography is the primary technique to assure data security. This scheme provides various factors to encrypt and decrypt the data using a key such as Lychrel numbers and RGB colors as the password. There are three keys used to provide secure and reliable data transmission with the RGB colors which is a primary security element which provides authentication. Here colors and Time based one-time key are been used as the password for authentication process. Lychrel numbers are used to encrypt and then decrypt the data that is to be transmitted.

Keywords: - RGB colors; Lychrel numbers; Time-based one time password; AES algorithm

I. INTRODUCTION

Security has been a great importance in all aspects. In case of considering the network security, many passwords have been used. There comes a lot of style in creating the password. That security is done by the usage of RGB colors and Lychrel numbers. The first level of security is been provided by using the user login and the next is done by the RGB colors and mainly the message is encrypted using the Lychrel numbers. This enhances a high level of security by providing no loss of data. Hackers have less probability to attack the data send by this type of security. When colors are used as one of the parameter in case of password it's very difficult to identify the password. Because in case of RGB colors there are more sets of passwords can be set. So it is not so easy to find the password. After that the message encryption and decryption is done by the Lychrel numbers.

II. MOTIVATION

.Nowadays data loss and hacking is growing in a rapid manner. To say for example many Facebook ID has been hacked daily. To have a secured data transmission there should be some way or technique to send the data. Another day to day example is, when we send a mail that should not be eavesdropped or hacked by anyone else except the sender and the receiver. So the encryption and decryption should me more difficult. So this technique using RGB colors and Lychrel numbers, one time password using the AES algorithm will improve the security issues. The scope of the project is very high because the data security is more important everywhere. But the main issue is that it should be more secured from the hackers. Some of the techniques can be easily hacked by the hackers. But in this technique it is hard and difficult for the hackers to find the actual data that is to be sent.

III. RELATED WORKS

Many of the cryptographic algorithms have been studied and proposed in this paper. Here there is a use of RGB colors which itself make the message transmission even more secured. Further the Lychrel number which acts as a key to encrypt and decrypt the actual message is worse hard to find. The other security factor is the Time-based one time key which is generated at the time of login. . In the survey given by Mohammed Abutaha all types of cryptographic techniques is given. But where the use of RGB colors, Lychrel numbers and Time-based one-time password is not combined together and used. By combining al the three factors which have a wide range. So it is difficult to find even a single factor. In Maxwell theory color cryptography has been enhanced.

IV. EXISTING SYSTEM

In Secret Key Cryptography technique the key which is used is known only to the sender and the receiver. So it will be secured but only some of the keys are made secret. This is also called as symmetric encryption and decryption. The same key is used to encrypt and decrypt process. Only the authenticated users can use the private key and can access the necessary information. In Public Key Cryptography technique the key which is been used is known to all the users. Not all the keys are made public only the necessary keys are made public. This is also referred as asymmetric key cryptography. By using the public key the information which is made public can be accessed by all the users. A hash function will be used and the key values will be generated using the hash function. A hash table is been maintained for this values to be generated. It is difficult to find but the maintenance of the hash table is difficult. Maintaining hash tables needs more memory space. So the space complexity increases. An Armstrong numbers [1] is used here where it is the addition of cubes of digits in the number which is equal to its original number. But till 5000 there are only 5 Armstrong are there so the hackers can easily find this. Armstrong is known to all and it is used widely in the mathematical and in the security process. There are several more algorithms and techniques [9] like Bach's algorithm, Common Scrambling Algorithm, Fuzzy extractor, Mental poker, Verifiable random function etc.,

V. OUR APPLICATION SCHEME

In this scheme we propose a different approach for providing the security of the data's. Here few factors are been used such as RGB colors [3] [4], Lychrel numbers and the Time-based one time password [5]. Initially when a user login to send the data they will receive a onetime password to mobile. By using this user can login to send the data. Later again each user uses their own RGB color to provide more security. Finally Lychrel number is been used to encrypt and decrypt the data using the AES algorithm.

A. ***System Design***

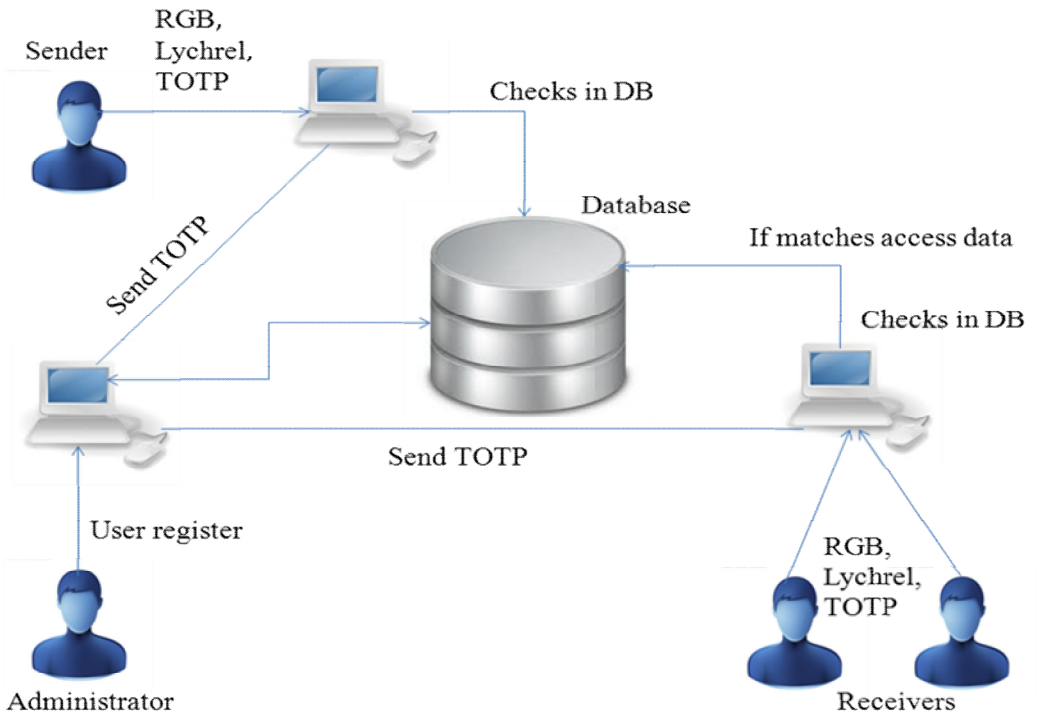

Figure 1. System Design

B. ***Time-Based One Time Password***

TOTP is a time based password [6] factor, where a new password is generated at a particular time. That password will be used for a particular interval of time say for 40 seconds. After that time interval a new password will be generated.

C. ***RGB Color***

RGB color a combination of red, blue and green color which are the basic primitive colors. There are about 16.7 million colors which are formed using the RGB. It is represented using the triplet value either arithmetic or percentage or 8 and 16 bit formats.

D. ***Lychrel Number***

Lychrel numbers are formed using the iterative process of reversing the digits and making a sum of those digits where the resulting number should not form a palindrome. Several numbers form a palindrome through this process. It is very difficult to identify which lychrel number has been used. The smallest lychrel number is 196. Here we can consider the example as e-mail. A user can login to send a mail and receive the mail. At the time of login a time based one-time password is generated and that is been sent to the mobile phone. The extra password is given which is the RGB color value. Each user will have own RGB code. Only the authenticated person can know the RGB colors and the key to decrypt those codes. So providing this much of security factor will greatly enhance the necessary security in the process of message transmission. The same is decrypted at the receiver side. Fig 1 tells the overview of the system.

E. ***Encryption***

- Each letter of the actual message or data which is to be transmitted is assigned to its equivalent ASCII values. Use any of the Lychrel number which is added with the ASCII values. The Lychrel number is added by squaring each of the digits in the number. Say for example the number be 196 then it is used as

  1 9 6 1 81 36 1 6561 1296 1 9 6
- The resulting set of values is stored in the matrix form which is of m x m form. A encoding matrix is formed by using the Lychrel number which is used for adding with the ASCII values. For example,

consider 196 as Lychrel number, and then the encoding matrix will be formed. This method is done by the AES algorithm [7]. Then both the matrix are multiplied and the encrypted set of values are got, which is the values of actual message and stored in the database.

F. ***Decryption***

The reverse of the Lychrel number is the key used for decryption process of the actual message. Time based one-time password is been separately used for the receiver side. The receiver also uses the unique RGB color which is been used to identify it. When all the three factors are correct the actual message can be viewed. Even a single factor is not correct the data cannot be viewed.

VI. CONCLUSION

To provide the necessary security in the field of data transmission we propose some security key factors. Thus providing with all these factors the level of security is been enhanced. All the three factors and also with the initial login it is very difficult to find all the factors thus it provides the necessary security. Lychrel and the RGB factors are much difficult because the probabilities of the factors are very high, since there are lot of combinations in both the factors. In the future work the data can be analysed which is original or not.

REFERENCES

[1] Prof. Mr. S. A. Saoji, Nikita B. Agarwal, Mrunal B. Bokil, Ashwini V. Gosavi, "Securing e-mails using colors and armstrong numbers", IJSCER, vol 4, pp 1438-1440, July 2013.
[2] Kamlesh Gupta, Sanjay Silakari, "ECC over RSA for Asymmetric Encryption: A Review", IJCSI, vol 8, pp. 370-375, May 2011
[3] Mazzeo, Giove, Moramarco.G.M, Spagnolo P, "HSV nad RGB color histograms comparing for objects tracking among non overlapping FOVs, using CBTF",IEEE AVSS, pp. 498-503, Sept. 2011.
[4] Jeahwan Park, Woosung Kim, Hyeon-Joong Yoo, Youngbum Jang, "From detecting to recognizing color codes", IEEE ICATC, vol. 3 pp. 2230, Feb 2006.
[5] Song Luo, Jianbin Hu, Zhong Chen, "An identity based one time password scheme with anonymous authentication", IEEE NSWCTC, vol. 2, pp. 864-867, April 2009.
[6] Wen-Bin Hsieh, Jenq-Shiou Leu " Design of a time and location based one time password authentication scheme", IEEE IWCMC, pp. 201-206, July 2011
[7] Fei Shao, Zinan Chang Yi Zhang, "AES encryption based on the high performance computing of GPU", IEEE ICCSN, pp. 588-590, Feb. 2010.
[8] Yuan Kun, Zhang Han, Li Zhaohui, "An improved Aes algorithm based on chaos", IEEE MINES, vol. 2, pp. 326-329, Nov. 2009.
[9] Ayoub F, Singh K, "Cryptographic techniques and network security", IEEE proceedings, vol. 131, pp. 684-694, Nov. 2008.

Authors Profile

R.VANATHI received her B.E (CSE) Degree from Info Institute of Engineering, Coimbatore, Tamil Nadu, India and pursuing M.E (CSE) Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her field of Interest are Cryptography and Network security, Database Management System and Operating System.

L.DHANAM received her B.E (CSE) Degree from Info Institute of Engineering, Coimbatore, Tamil Nadu, India and pursuing M.E (CSE) Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her field of Interest are Network security, Operating System and Theory of Computation.

K.R.SENTHILNATHAN has obtained his Post Graduate degree, M.E.(Computer Science and Engineering) in Nandha Engineering College, Erode and obtained his Graduate degree B.E., (Computer Science and Engineering) from Velalar college of engineering and technology, Erode. He is currently serving as Assistant Professor of Department of Computer Science and Engineering at Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu with a teaching experience of 2.5 years. He is specializing in the area of Compiler Design.

M.S.VINU has obtained her Post Graduate degree, M.E.(Computer Science and Engineering) in Nandha College of Engineering, Erode and obtained her Graduate degree B.E., (Computer Science and Engineering) from VSB College of Engineering, Karur. She is currently serving as Assistant Professor of Department of Computer Science and Engineering at Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu with a teaching experience of 2 years. She is specializing in the area of Network Security

