MULTILEVEL AUTHENTICATION USING GPS AND OTP TECHNIQUES

Priyanka R. Tope[1], Pranali R. Raut[2], Swamini B. Dalvi[3], Archana C. Lomte[4]

[1, 2, 3]*Student,* [4]*Assistant Professor, Department of Computer, BSIOTR (W), Maharashtra, India*

Abstract

Location based authentication is a new direction in development of authentication techniques in the area of security. In this paper, the geographical position of user is an important attribute for authentication of user. It provides strong authentication as a location characteristic can never be stolen or spoofed. As an effective and popular means for privacy protection data hiding in encrypted image is proposed. In our application we are providing secure message passing facilities for this OTP (One Time Password) and Steganoghaphy techniques are used. This technique is relatively new approach towards information security.

Keywords: *Location based authentication, GPS device, Image encryption, Cryptography, Steganography, and OTP*

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

1. INTRODUCTION

Nowadays, in many papers main discussion is on user's location for authentication. Authentication is any process by which a system verifies the identity of user who wishes access it. It is normally based on identity of user such as user ID and password. Authentication is one of the three main processes of AAA systems (Authentication Authorization Accounting)[1].

Location based authentication is a latest technique for providing higher security. It provides wireless technologies for sending secure message. Using location based authentication we find the user's geographical position. For this we are using three factors: Latitude, Longitude, and Altitude. Example of location based authentication such as Corporate mail, military area, banking etc.

Consider the example of any social networking site; the important information about users such as user-name, password, personal details, etc. is stored in the database. This database is mostly placed on server which is located at particular location. Access to this should be granted only when the person is at geographic position where the particular server is located. Location Based Authentication not only consider user ID and password but also take geographical position; thus leading to higher level security. After successful authentication, the data that is to be sent and received would be encrypted. To achieve this Advanced Encryption Standard (AES) algorithm will be used.

1.1 Steganography

Steganography is the art and science of writing hidden messages in such way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

As access to powerful computers increases, delivering information with digital data becomes more convenient on the internet. When these digital data are sensitive-whether text, image or video-there is concern that the information

To enhance the security of information communication, the digital data is embedded into other irrelevant products as secret data. A method call steganography, popularly used with internet communication [2], embeds secret data in a stego-image that looks like a photograph. After the stego-image is transmitted, the authorized receivers recover the secret data using a spatial scheme, while attackers do not realize that the stego-image hides secret information at all. The least significant bits (LSBs) method is a well known steganographic method. Wang et al. [3] proposed a substitution scheme using LSBs that improved the stego-image's quality.

1.2 One Time Password (OTP)

A One Time password (OTP) is a password that is valid for only one login session or transaction. OTPs provides strong authentication for remote access such as high level IT resources, web service, mail server, online transaction. The most important shortcoming that is addressed by OTPs is that, the contrast to static password, they are not vulnerable to replay attacks. On the down side, OTPs are difficult for human beings to memorize.

2. SYSTEM ARCHITECTURE

This Software will work as a communication medium for the members of an organization who wants to secure their data transfer from being stolen. The tool is designed to work on a network. The one who is going to use the software can work in any environment condition provides all the tools required executing the file. The machine on which the operation takes

place should have basic Windows Operating System (XP/2007 or higher).

In our application we are provides secure message passing facilities:

1. Secure Authentication
2. Sending message of generated (OTP) password to user mobile
3. Generation of strong key i.e. one time password
4. Encryption of secure data
5. Embedding in image (interested region)
6. Decryption of data
7. Message sending

Three level authentications is necessary for customer

1. Normal Login
2. OTP (One Time Password)
3. Location Based Login

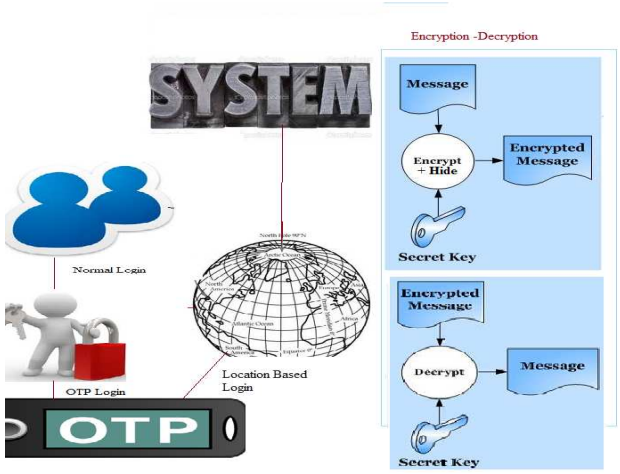

Fig -1: System Architecture

3. ALGORITHM

In this paper we are using following algorithm:

3.1 AES (Advanced Encryption Standard):

AES algorithm is published in 2001[4]. In this algorithm block length is limited to 128 bits and the key size is specified to 128, 192 or 256 bits.

Table -1: Key Size

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/156
Number of rounds	10	12	14
Expanded key size (words/byte)	44/176	52/208	60/240

AES Algorithm Steps:

- Substitute Bytes: Plain text will be written in matrix format. For each byte a new byte will be substituted and a new matrix will be formed.
- Shift Rows: First row is kept as it is. second row is shifted left by one column and so on.
- Mix Columns: In mixed column, shift row matrix will be multiply with another fixed polynomial matrix to get mixed column matrix
- Add Round Key: Round key is added to the state using x-or operation

3.2 ROI (Region of Interest):

This algorithm is used for steganography. For this ROI algorithm is used and the data can be hidden in the region of interest of the cover image.

ROI Steps:

- Input cover image
- Input text data
- Select ROI region
- Read input cover image
- Get bytes of text data
- Hide data into cover image using ROI
- Generate stego image as a output.

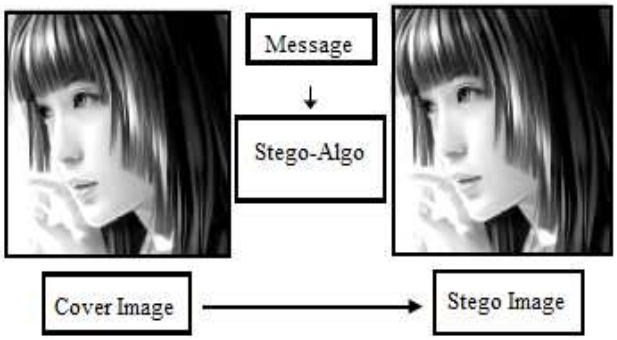

Fig -2: Image Steganography

4. IMPLEMENTATION

In this working phase user have to follow the three login steps such as textual login, GPS login, and OTP login In first part, when user perform normal login if it gets fail then user is not valid but if it will get success then it goes to perform next type of login i.e. GPS login. In this it get success then it follow the next type of login is the OTP login. If OTP login gets success then it perform the operation such as enter data for that we are going use encryption and ROI steganography and encryption of data will be takes place. At the server database decryption of encrypted data will be takes place .Simultaneously GPS parameter also check if the user is not in valid area then it is

not a valid user but if user in valid area then data will get extracted from image then decryption of data will be takes place and user get original data.

CONCLUSIONS

Location dependant authentication is an additional factor in providing strong authentication. It gives owner the complete control of the information that only he has access to. The software will perform its functions properly only when the user is within the authorized range. So the software will meet the all security issues like confidentiality, integrity and so on. Hence this application will be most suitable for military and industrial data. The authentication techniques where theoretically proposed till now.

REFERENCES

[1]. H.Rui, Y.Man, H.Janping, K.Zhigang, and M.Jain," A novel service-oriented AAA architecture," in Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on, 2003, pp. 2833-2837 vol.3.

[2]. S. Zhen, L. Zhoujun, and D. Wenhua, "Different approaches for the formal definition of authentication property, "in Communications, 2003. APCC 2003.The 9th Asia-Pacific Conference Communications, 2003, pp.854-858 Vol.2.

[3]. A. Menezes, P. Van Oorschot, ands. Vanstone., Handbook of Applied Cryptography: CRC Press.1997.

[4]. A simplified AES algorithm and its linear and differential.

[5]. Jhon Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", International Journal of Soft Computing and Engineering(IJSCE)ISSN: 2231 2307, vol-2, issue-1, March 2012.

[6]. E. Denning and P. F. MacDoran, " Location-Based authentication: Grounding cyberspace for better security",Computer Fraud and Security, vol.1996,pp.12-16,1996.

[7]. P.S.Tikamdas and A.El Nahas, "Direction-Based proximity detection algorithm for location-based services",in Wireless and Optical Communications Networks,2009. WOCN'09. IFIP International Conference on,2009,pp.1-5.

[8]. B. Schilit , J. Hong, and M. Gruteser, "Wireless Location privacy protection", Computer, vol.36,pp.135-137, dec 2003.

[9]. Moreland T, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privatech.pdf.

BIOGRAPHIES

Priyanka R. Tope, Department Of Computer, BSIOTR (W), Pune, Maharashtra, India. Email-id- tope.priyanka123@gmail.com

Pranali R. Raut, Department Of Computer, BSIOTR (W), Pune, Maharashtra, India. Email-id- pranaliraut77@gmail.com

Swamini B. Dalvi, Department Of Computer, BSIOTR (W), Pune, Maharashtra, India. Email-id- swamini.dalvi7@gmail.com

Prof. Archana C. Lomte, Department Of Computer, BSIOTR (W), Pune, Maharashtra, India. Email-id- archanalomte@gmail.com