ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 7, January 2015

Three Factor Authentication using Location

S.S.Mule, Chitra Raskar, Yogita K.Bhor, Archana Marne, Vishalsingh Nikumbh
Asst. Prof, Research Scholar, Research Scholar, Research Scholar, Research Scholar
Department of Information Technology, MMIT College, Lohagoan

Abstract*— Verification is the process of identify correct communicating entity and giving right to use to valid users. With the increase of wireless technologies in sector like the military, banking, aviation, etc, there is a need to verify the validity of a genuine user. In this paper, we are explain how location can be used as one of the permit to give right to use of data only to genuine user. To distinguish our work from existing ones we are using GPS technologies as well as we take advantage of the ubiquity of IEEE 802.11 WLAN (Wi-Fi) to compliment blind spots of GPS location sensing. The location-based authentication (LBA) using GPS and Wi-Fi is a quite new direction in the information security. The direction gain an importance nowadays due to movable devices coming to wireless network environment.

Index Terms—**GPS, Location based Authentication (LBA).**

I. INTRODUCTION

Today's information systems require clear classification between communicating entities (often entities are users). Procedure of entity recognition is in general called verification The authentication is defined affirmation of the identity of certain object in centralized systems, as refers [1]. More generally, authentication can be referred as message origin validation. In general, authentication can be classified into two categories: 1) location independent, 2) location dependent. If authentication is location independent then any one can access powerful data from any location, there is chance of misuse of highly aware information specifically hackers can hack data from any location. Which is risky for highly protected data like military data or company data which are not permitted to take outer the assured premise

.This motivate us to design a location based authentication to protect highly secure information. The existing verification models are most prevalent verification models and have been used for decades. These models use aspects having factors like: password, digital certificate, and biometrics. LBA is a technique that will take into account environmental location of user which is latitude, longitude & altitude of the person who is trying to validate his uniqueness. Location information is capture at the case in point when he is trying to right to use his mail account. The users get access to his mail account only after estimation of following 3 credentials:

1. User id & Password
2. One Time Password
3. Location.

Thus after this we can make a decision whether the user is genuine or not. Access to the information should be approved only when the person is at registered geographic position or else access must be denied. In other words information should not allow to taken away outside the premises. GPS technology or Wi-Fi is detected geographic position. GPS uses line of sight to satellites, so it does not work when a user is indoors or in other circumstances when the line of sight is obscured.

Therefore, we choose another approach – Wi-Fi, to find the “blind” spots of GPS location sensing. After successful authentication the data that is to be sent and received would be encrypted and hide behind the stego-image. To perform this Advanced Encryption Standard and Least Significant Bit algorithm should be used.

II. RELATED WORK

Authentication is accepting validating of identity of a person to decide whether he is legitimate user or not. For this earlier two factor authentication technique is common in use. In the two factor authentication individual can be identified by his user name and password. If username and password is matched then process of authentication is done and user can access the data. User is looking for a password that is easy to remember and secured from any attack but when user has different accounts it is not an easy task. But in this technique anyone can hack password and access information. In cases in which user’s passwords are stored in encrypted form on the server machine, plain-text passwords are sent across a possibly-insecure network from the client to the server. Anyone can access to the intervening network may be able to “snoop” pairs out of conversations and replay them to forge authentication to the system. For more security new factor is added i.e. location. Relocating is the first step to provide location of a user. common locationing technologies include GPS, Wi-Fi, cellular, Bluetooth, too name of few .the applicable environment for these technologies varies and their locationing accuracy also increases, so there has been a great deal of researches aiming at improving the two factors. Using a location technology, NI et al. [2] improved the locationing accuracy of RFID by deploying reference tags in the field. Accuracy of Location can also be improved by combining two or more technologies.

Based on the findings of [3], we are motivated to improve the location sensing capabilities of mobile devices, to make location-based authentication. Encryption is the conversion of data into a form, called an encrypted data that cannot be easily understood by unauthorized people. Decryption is the process of get original information. Decryption key is required. After Encryption encrypted information is cover behind a image called Stego-image and Process is called as Stenography. Using both we make information unfeasible for an unauthorized user. However, we can get better dependability and protections of the authentication mechanism by combine several authentication factors into a distinct representation. It shall also be noted that even though there are a few location-based authentication techniques, those techniques go through from the difficulty of incorrect locationing in case of unsighted spot of GPS technologies. To get better this we are combining GPS and Wi-Fi for perfect location.

III. PROPOSED SYSTEM

The main of the project is to focus on security of communication channel and data of industrial and defense services which are location dependant. That is user can have access to data only when he is in predefine range of particular area. To authenticate users, following credentials will be used:

A. Location

Location of a specific user is highly sensitive information. This can be used for efficient authentication. This can be used as one of the key attribute to authenticate a person. In this model we will be using GPS technology and Wi-Fi technology.

a) GPS technology

GPS receiver for tracking the geographic position of a particular user. The task of GPS device is to track the latitude and longitude co-ordinates of a user who is trying to get authenticated. Once the location sent by the user is process by server, he will be access his mail account. One user can have multiple locations depicted.

b) Wi-Fi technology

Specifically, GPS uses line of sight to satellites, so it does not detect user location when user is in other circumstances when the line of sight is obscured. Therefore, we choose another approach for this type of situation i.e. IEEE 802.11 WLAN, to compliment blind spots of GPS location sensing. Wi-Fi has been especially deployed around the world. In many cases, more than ever in urban areas it is very likely for a WLAN client to find out multiple APs when scanning for wireless links therefore, in our design we allow multiple(2 APs) APs to be connected with one location, to enhance accuracy of locationing.

B. One Time Password

One Time Pass-word is a password system where passwords can only be used once and the user has to be authenticated with a new password each time. This guarantee the safety even if an attacker is tapping password in network or a user loses it. Besides, OTP features portability, and extensity enables to keep the information from being leaked.

C. Encryption

The method of converting simple message to secret message is known as encryption. In this system the data that a valid user will send or receive will be in unreadable form. To attain this we will be using AES (Advanced Encryption Standard) algorithm which is advanced version of DES (Data Encryption Standard).The main advantages of AES are that its conflict against all known attacks; speed and code density on a wide range of platforms; design simplicity.

D. Stenography

The steganography can be considered as a branch of cryptography that tries to hide messages within others, avoiding the perception that there is some kind of message. To apply steganographic techniques cover files of any kind can be used, although archives of image, sound or video files are the most used today. Similarly, information to hide can be anything: text, image, video, sound, etc.

IV. ALGORITHMS

A. For Encryption and decryption (AES algorithm)

AES is Advanced Encryption Standard. 64 bit block size. Key size -128, 160, 192, 224, 256 bits. The algorithm begins with an Add round key stage followed by 9 rounds of four stage and a tenth round of three stages. This apply for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the opposite of its matching part in the encryption algorithm. The four stages are as follows:

1. Substitute bytes

This is a byte-by-byte substitution. The substitution byte For each input byte is found by using the same lookup table. The size of the lookup table is 16*16. To find the substitute byte for a given input byte, we divide the input byte into two 4-bit patterns, each yielding an integer value between 0 and 15. (We can represent these by their hex values 0 through F.) One of the hex values is used as a row index and the other as a column index for reaching into the 16*16 lookup table

2. Shift rows

The Shift Rows transformation consists of (i) not shifting the firs row of the state array at all; (ii) circularly shifting the second row by one byte to the left; (iii) circularly shifting the third row by two bytes to the left; and (iv) circularly shifting the last row by three bytes to the left

3. Mix Columns

This step replaces each byte of a column by a function of all the bytes in the same column.

•More precisely, each byte in a column is replaced by two times that byte, plus three times the next byte, plus the byte that comes next, plus the byte that follows

4. Add Round Key

- XOR state with 128-bits of the round key
- Again processed by column (though effectively a series of byte operations)
- Inverse for decryption identical since XOR own inverse, with reversed keys.
- Designed to be as simple as possible
  - A form of Vernam cipher on expanded key

-requires other stages for complexity / security

B. *For Stenography (LSB Algorithm)*

LSB is least significant bit.
Used to find the last bit of every byte where the message bit is stored.
Steps-

1) Convert message into binary form.
2) Select suitable cover image to embed message.
3) Find LSB of cover image.
4) Insert message bit into LSB of cover image.
5) Stego image.

V. EQUATIONS

Location Based Authentication Algorithm Mathematical Module:

1. User (U) this is actor handles system functionality.

SET OF U= {1.......N}

2. Capture GPS Co-ordinates of User Device Lat and Longi factor.

2.1 Get Stored Location Co-ordinates Lat and Longi factor.

2.2 Calculate Distance between capture Co-ordinates and Stored Co-ordinates to define the periphery i.e. certain range within which user can get access to the data.

Formula-

Var phi1=lat1 to radian ( )

Var phi2= lat2 to radian ( )

Δlambda= (long2-long1) to radian ( )

Doubledist=Math.sin(phi1)*Math.sin(phi2)+Math.cos(phi2) *

Math.cos(Δlambda);

Output = Find Nearest Location.

VI. CONCLUSION

Location based authentication is an additional factor in providing strong authentication as a location characteristic can never be stolen or spoofed. It has provided a supplementary dimension in network security. It gives the owner the complete control of the information that only he has access to. We are improving Locationing accuracy by combining two or more locationing technologies GPS and Wi-Fi. To distinguish our work from existing ones we are using GPS technology as well as we takes advantage of the ubiquity of IEEE 802.11 WLAN (Wi-Fi) to compliment blind spots of GPS location sensing. We are providing security over communication channel by encryption and stegnography .Message send and received by user will be first encrypted and then would be covered behind a image called stego image. This will give extra security to the user while communication channel.

VII. FUTURE WORK

The avenues for future work on this application are:

1) Monitoring behavior of the user.
2) Implementation on a PDA.
3) Besides latitude and longitude fields, an altitude field can also be added.

REFERENCES

[1] Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, "Location Based Authentication: A New Approach towards Providing Security," International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153.

[2] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "LANDMARC: Indoor Location Sensing using Active RFID," Wireless Networks, vol. 10(6), pp. 701-770, 2004.

[3] T. Sohn, K. A. Li, G. Lee, I. Smith, J. Scott, and W. G. Griswold,"Place-Its: A Study of Location-Based Reminders on Mobile Phones," Proc. 7th Int'l Conf. Ubiquitous Computing (UbiComp2005), LNCS 3660, pp. 232-250, Sep. 2005.

[4] Chi-Yi Lin, Ming-Tze Hung, and Wei-Hsun Huang, "A location-based Personal Task Management Application for Indoor and Outdoor Environments" 2012 15th International Conference on Network-Based Information Systems.

[5] Rahul Joshi, Lokesh Gagnani, "Improve Security & Quality of Stego Image Using Proposed LSB Method," International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 3, May-Jun 2013, pp.1291-1294.

[6] Salony Pandey, Prof. Amit.M.Lathigara, "Hiding Text behind Image for Secure Communication," International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 3, May-Jun 2013.