International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Live Interactive Authentication using Remoting Techniques (L.I.A.R)

[1] Rakshit Ogra [2] Namrata Shivanekar [3] Pawan Deshmane [4] Sanket Godbharle [5] Prof. H.K Kaura
[1][2][3][4][5] Department of Information Technology
Fr. C. Rodrigues Institute of Technology, Vashi
Navi Mumbai, India
[1] ro3184@gmail.com [2] namratashivanekar@gmail.com, [3] pawandshmn@gmail.com
[4] sanketgodbharle10@gmail.com [5] hkkaura@gmail.com

Abstract- **The process of authorizing an individual is usually based on username and password and also by using message based system. A remote authentication system is handled generally through remote systems itself without any manual / operator assistance. Presently there are many authentication mechanisms deployed on various applications on the internet which deal with financial transactions. In a transaction involving payment through credit card, authentication involves entering credit card, authentication involves entering credit card number, name on the card, Card Verification Value (CVV) number, expiry date. Further to this OTP (One Time Password) is used in which person to be authenticated can have access is required to enter a code which is provided by remote systems to user on his mobile phone. CAPTCHA (Completely Automated Procedure to Tell Computers and Humans Apart) is used for the authentication. The proposed system is an interactive remote authentication system which can be deployed in addition to the broadly available authentications only for high value and critical financial transactions. This involves verification / authentication of remote user by human operator on the authentication system-end. This involves two levels of authenticating remote user. At the first level remote user is asked to capture his image using webcam or any other camera (Mobile) and then send the image to the system. The human operator on system-end verifies the captured image of the remote user comparing it with the image stored in the system database. If it matches, the second level of verification is initiated by human operator. Human operator will ask the remote user to perform some action such as turn face left, right or up, touch your nose, remove the cap, etc. and capture the picture of his modified face as per an instruction and send to human operator. If the new image is as per an instruction of human operator that verifies the remote user is authenticated.**

Keywords: ***Authentication, remote, verification, operator*****.**

I. INTRODUCTION

1.1 Background

Authentication means verifying the identity of someone (a user, device, or an entity) who wants to access data, resources, or applications. Validating that identity establishes a trust relationship for further interactions. Authentication also enables accountability by making it possible to link access and actions to specific identities. Many consumers have started to put faith on these organizations which guarantees products and services due to which there has been an increase in online transactions and the online market has been now valued in trillions.. But there have been disadvantages and flaws in this system. Increase in online transactions have also led to the rise of increased issues of hacking and stealing which has made developers to think of undertaking various security measures to tighten up the security in the unknown waters of Internet. OTP (One-Time Password)[1], Biometric systems[2] (face, voice recognition, fingerprinting.) are all popular authentication mechanisms deployed on various systems but they have been cracked and their flaws have been exposed on various occasions which has led to the increase in the need for a change in existing systems. Our proposed system of authentication focuses on following steps. Capturing the user's image and checking with stored image by human operator and authenticating the user by carrying out live interaction with him/her. While signing in system, user has to capture his/her image and send to human operator on system side which he will compare the image. Human operator at system-end will manually check the new image with already stored image in database. If they are same then only next step will be activated. Human operator will ask the user to do random physical action such as turn face to left, turn face to right, etc. Then take the picture by webcam or mobile. After getting new image with action performed human operator will again check the image manually. If the current image is as per the specified physical actions then only user will be authenticated and allow to get access to do transactions.

1.2 Motivation

The real motivation of choosing this project topic was to create a new authentication system using a combination of existent systems as well as utilizing the flexibility and platform independence of the currently

available technologies. Also, due to some shortcomings in the existing systems, there was the need to innovate and create a new platform for authenticating the users in order to achieve safe and secure authentication

This research aims to study the existing authentication systems and to design and develop an improved mechanism, to empirically test its security & usability, and to compare it with existing deployed schemes. The extent of previously discussed problems and their effect on individuals and organizations give raise to a number of research questions:

- What is the security and usability performance of authentication systems in actual use?
- Are facial recognition schemes as reliable as credit card credentials or OTP and CAPTCHA schemes?

This research will provide secure, reliable user authentication mechanisms to help the users who carry out online transactions. It is a better authentication method which cannot be easily manhandled by an unauthorized user.

1.3 Scope

Live Interactive Authentication Using Remoting Techniques is a system that will be developed for users who want to get authenticated while carrying out online financial transactions. With the help of this system, the reliability of authenticating a user increases. This system can be used in addition of already implemented authentication methods like OTP(One-Time Password).The scope of this project is to design and implement a new, efficient, robust and highly secure remote authentication system which will authenticate the users through the means of any deployed image capturing device on the computer or mobile. The main reason behind this project idea was to eliminate/minimize limitations and flaws in the currently existing and deployed authentication mechanisms and to place a new system which could provide the users with a more secure, robust and reliable way of authenticating themselves. This system when deployed, will help to prevent any fraudulent financial transactions carried out by the hackers and therefore will help to save the data integrity and will also eliminate the heavy loss of money of the original users.

1.4 Issues and Limitations3

- Both the user and human remote operator have to present and attend the session at the same time.
- If the user suffers from any kind of changes in facial anatomy due to age or accidents, then the human operator will face difficulties to identify the user.
- This method is expensive for carrying out small-value transactions.

II. LITERATURE SURVEY

There are many different authentication systems are present that we can use in day-to-day life. But One Time Password is most widely used than any other authentication systems. CAPTCHA schemes is also used with password to check whether system is used by human or a machine. There are existing remote authentication systems which are discussed as follows. A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access. Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. Existing password authentication schemes can be categorized into two types: weak-password authentication schemes and strong-password authentication schemes. When compared to strong-password schemes, weak-password schemes tend to have lighter computational overhead, the designs are simpler, and implementation is easier, making them especially suitable for some constrained environments.

A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and, through text-to-speech conversion, to any mobile or landline telephone, text messaging has a great potential to reach all consumers with a low total cost to implement. However, the cost of text messaging for each OTP may not be acceptable to some users. OTP over text messaging may be encrypted using an A5/x standard, which several hacking groups report can be successfully decrypted within minutes or seconds, or the OTP over SMS might not be encrypted by one's service-provider at all. In addition to threats from hackers, the mobile phone operator becomes part of the trust chain. In the case of roaming, more than a single mobile phone operator has to be trusted. Anyone using this information may mount a man-in-the-middle attack. A card security code (CSC), (also called card verification data, card verification number, card verification value, card verification value code, card verification code, verification code (V-code or V code), card code verification, or signature panel code (SPC) are different terms for a security feature for "card not present" payment card transactions instituted to reduce the incidence of credit card

fraud. The CSC is in addition to the bank card number which is embossed or printed on the card. The CSC is used as a security feature, in situations where a PIN cannot be used. The PIN is not printed or embedded on the card but is manually entered by the cardholder during a point-of-sale (card present) transactions. Contactless card and chip cards may electronically generate their own code, such as CVV or Dynamic CVV[4].

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour /scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

III. PROPOSED SYSTEM

We propose a reliable remote based authentication system under the name (L.I.A.R) which will be using live interaction with the users remotely using Internet as a medium for authenticating them[5]. This project will consist of two phases in the process of authenticating the user using webcams and live image sharing mechanisms.

- Capture of user facial image and manual checking of the captured photo by the remote manual authenticator using the stored photo of the same user in system database.
- Authenticating the user by carrying out live interaction (through checking and verifying of physical actions as ordered by the remote authenticator) with that user.

3.1 Image Checking:

Suppose a user is carrying out a high-value online transaction on a bank website or any other website, he has to enter all the necessary credentials of the credit card as the first process and then has to follow the OTP procedure to get through the transaction. Our system will be deployed in addition to the OTP service and it will need a basic webcam and HTML-JavaScript support to access the system. In the first phase, a secure connection will be established between the user and a remote authenticator situated at random location and also allocated randomly. Through that secure connection, the remote authenticator will be able to view the images sent by that user and will be able to transmit messages to the client for the live interaction. The user will be clicking an image of himself and will be sending to the remote authenticator who will be cross-checking with the stored image stored in the database manually. This manual checking of the image will be the first step in our system and will confirm whether the user is the correct registered user or not.

3.2 Live Interaction:

After the image checking phase, the remote authenticator will instruct the user through live text sending. The user will be told to perform certain simple and feasible actions such as "Turn left", "Turn right", "Show a V symbol" etc. These actions will be viewed by the remote manual authenticator through the images sent by the user in which the actions will be recorded and will be confirmed to authenticate and complete the transaction, if and only if, the actions are as per the request. If the actions are not as per demanded, then the remote authenticator has full right to cancel the entire transaction process. This phase will determine whether the correct user who is carrying out the transaction is a live person or not.

IV. DESIGN

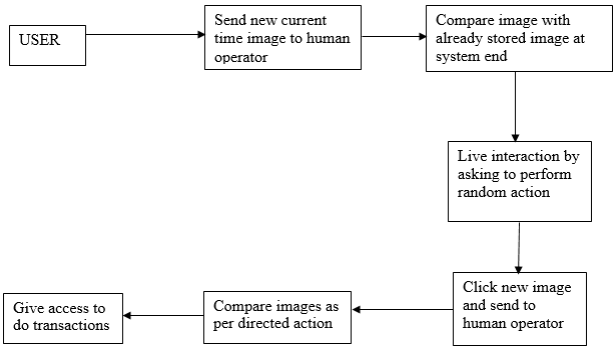

Fig. 4.1 Flow Chart Diagram

- To send new image at current time to remote side from the user who wants to get authorized.
- Image is compared with an already stored image at the remote end.
- User is asked to perform random actions according to instructions given by the operator.
- If the current image is as per the specified physical action, then user would be authenticated and allowed to get access to do transactions.

V. SOFTWARE AND HARDWARE REQUIREMENTS

On Computer:
At user side:-

- A general purpose personal computer with basic configuration with a webcam with min 2 MP resolution

At server side:-

- A general purpose computer with basic processing capability along with access to the Internet with Microsoft .Net framework support.

Operating Systems supported:

- Various Linux distributions: Fedora, Red Hat, Ubuntu. etc
- Windows: XP/7/8/8.1/10

On Mobile:-

- Basic smart phone configuration with standard ROM, RAM, processor with Internet Access along with supported browser

Operating System:

- Android: 3.0 and above versions
- Windows
- iOS

VI. CONCLUSION

It is a secure way of getting authenticated as human operator performs live interaction with the remote user. It can provide alternative for the tedious procedure of approaching the bank for the authentication while registering and also answering multiple customer service calls. It will be very useful when it comes to carrying out high-value transactions on the Internet. It is very easy to deploy with minimum system configuration needed. It is very robust, efficient, and scalable than any other authentication system. It also eliminates flaws and limitations of current existing schemes and also will provide employment to the needy.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the contributions Dr. S.M. Khot, Principal of Fr. C. Rodrigues Institute of Technology, Prof. H.K. Kaura, H.O.D. of IT department, Prof. Archana Shirke, Coordinator of IT department and our co-guide Prof Suraj Khandare for their work on the original version of this document.

REFERENCES

1. Browser Fingerprinting and the Online –Tracking Arms Race" An IEEE paper on Fingerprinting biometrics " (http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race)

2. "An Insight into Fingerprinting" (http://www.ieee.org/about/technologies/emerging/fingerprinting.pdf)

3. "Authentication For Remote Logins(r login)" (https://docs.oracle.com/cd/E19455-01/805-7229/remotehowtoaccess-27053/index.html)

4. "AVISPA- An Automated Validation Of Internet Security Protocols and Applications" – by Alessandro Armando, David Basin, Jorge Cuellar, Michael Rusinowitch and Luca Vigno (http://www.ercim.eu/publication/Ercim_News/enw64/armando.html)

5. "RADIUS- Remote Authentication Dial-In User Service" (http://searchsecurity.techtarget.com/definition/RADIUS)

6. "Search Personal Authentication through Remote System For E-Transactions (SPARSE)" (http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6734913)

.