IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 5, May 2022

DOI: 10.17148/IJIREEICE.2022.10579

SECURED AUTHENTICATION USING IMAGE SHIELD PROTECTION AND DATABASE CRYPTOGRAPHY

Dr.Shanmugapriya P[1], Paul Sneka L[2], Shree G K[3] , Varshaa M[4]

Associate Professor, Saranathan college of Engineering, Trichy-21, Tamilnadu[1]

Department of Electronics and Communication Engineering, Saranathan college of Engineering, Trichy-21[2]

Department of Electronics and Communication Engineering, Saranathan college of Engineering, Trichy-21[3]

Department of Electronics and Communication Engineering, Saranathan college of Engineering, Trichy-21[4]

Abstract-Website security is the most important aspect in web technology. Data privacy and security is very important in all web applications. Secured Authentication is the key point to prevent the data access from unauthorized users. Existing Login Authentication is implemented by using unique username and password as text format. But this system faces huge challenges from hackers, network intruders where people get the user’s password easily by several hacking methods. Hence, this paper propose the system for secured login authentication system using image hotspot security The architecture for image hot spot is mainly used to avoid the unauthorized user assessing the system using various text intrusion techniques. Initially authorized user need to identify the exact hot spot from the image. The user is asked to click the exact point and to confuse the hackers for each hot spot clicked; the user uploaded image is generated with pre-defined password support so that hackers found difficult for accessing the password. Second step is once hot spot is clicked in an image the co-ordinates selected will be compared with the encrypted database co-ordinates value , hence the user need to choose the hotspot with intersecting points exactly which is allowed only for 3 attempts moreover the account will be blocked. In graphical password protection, the particular hot spot is allowed to click by using Contour-Tracing Algorithm Based on a Pixel-Following Method. Uploaded files will be stored in secured form using Steganography. Each file will be hiding in the image.

I INTRODUCTION

A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services such as career services. Online social network sites are web-based services that allow individuals to create a public profile, create a list of users with whom to share connections, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging.

There are many ways that hackers can benefit from a malicious app: (a) the app can reach large numbers of users and their friends to spread spam, (b) the app can obtain users’ personal information such as email address, hometown, and gender, and (c) the app can “re-produce" by making other malicious apps popular. The architecture used that is thimage hot spot is used to avoid the unauthorized user assessing the system and it also prevent from hacking the password. Steganography is also implemented to cryptographic data so that it increases the security of this data . In this method we first encrypt a message using substitution cipher method and then embed the encrypted message inside a JPEG image using DCT in frequency domain.

II LITERATURE SURVEY

Ying Li, Liping du[1] at “Asynchronous Challenge-Response Authentication Solution” –April 2019. In order to achieve secure authentication, an asynchronous challenge-response authentication solution is proposed. SD key, encryption cards or encryption machine provide encryption service. Hash function, symmetric algorithm and combined secret key method are adopted while authenticating.

Gamze Akman[2] at “ authentication mechanisms in secure messaging applications**” – June 2017.** Today, the increasing popularity of instant messaging applications has introduced some security measures. One of these security measures is the authentication activity that users need to make.

Ning Zhang, Xeumincheng[3] at “Message Authentication with Secure Channel Codes**” –December 2018.** In this paper, we investigate physical (PHY) layer message authentication to combat adversaries with infinite computational

DOI: 10.17148/IJIREEICE.2022.10579

capacity. Specifically, a PHY-layer authentication framework over a wiretap channel (W_1 ; W_2) is proposed to achieve information theoretic security with the same key.

Pradeep Atrey[4] at “A new secure authentication scheme for web login using BLE smart devices” –January 2021. Existing user authentication schemes used for login to a website are incapable of handling recent phishing attacks such as real time (RT) / control relay (CR) man in the middle (MITM) attack and attacks launched via covertly installed malicious browser extensions (MEs).

Yang Jinbo,S[5] at “A secure strong password authentication protocol**” – April 2021.** Nowadays, password-based authenticated protocol receives more and more attentions due to their convenience and practicality for service provider and end-users despite the user of passwords drawn from a space so small that an adversary might enumerate.

III PROPOSED SYSTEM

User authentication can be made secure by biometric or token based authentication techniques but they require special hardware for processing. The other easy to use authentication option remains the knowledge based technique. Authentication through this technique is improved by two approaches. In first, image hotspot schemes have been proposed, while in second approach schemes are suggested by co-ordinates cryptographic techniques. In this paper second approach has been taken for improving the security of traditional textual passwords. **Image Hotspot Security:** The architecture for image hot spot is used to avoid the unauthorized user assessing the system and it also prevent from hacking the password.Initially authorized user need to identify the exact hot spot from the image. In earlier algorithm nearly five hot spot is used. Since this process has high probability of finding the password, proposed system with one hot spot password is designed. The user is asked to click the exact point and to confuse the hackers for each hot spot clicked; a duplicate image is generated so that hackers found difficult for accessing the password. Second step is once hot spot is clicked a matrix with list of alphabet is displaced user need to choose the character with intersecting points.To make the process more difficult for hackers each time a new matrix is generated. In this method user created two passwords one is textual password and another one is graphical password. In graphical password particular hot spot is allowed to click by using segmentation algorithm spot from the image is compared and alpha numeric matrix algorithm used. **Image Steganography:** Steganography also can be implemented to cryptographic data so that it increases the security of this data .In this method we first encrypt a message using substitution cipher method and then embed the encrypted message inside a JPEG image using DCT in frequency domain. Proposed scheme uses alphanumeric character based passwords, therefore memorability results would be same as textual password scheme. The problem with alphanumeric passwords is that easy to remember passwords are easy to guess through dictionary attack. However, in the proposed scheme easy to remember passwords are not easy to guess due to password transformation layer. Proposed password transformation layer can also be used for other knowledge based authentication schemes for improving the security against dictionary and brute force attacks.

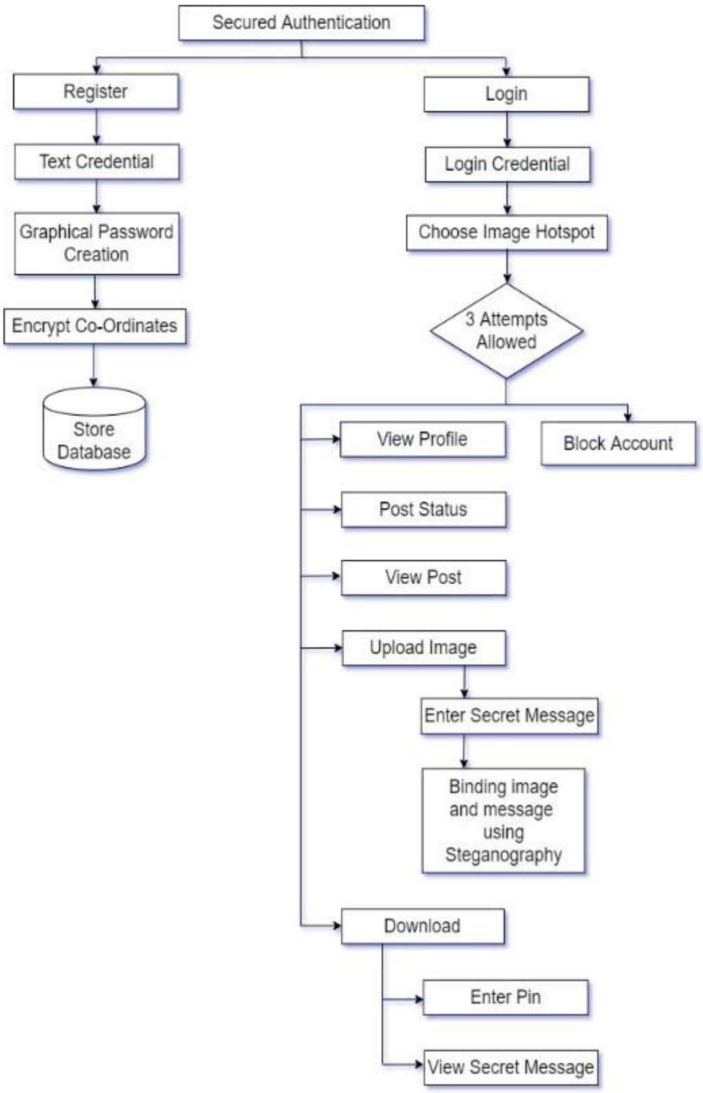

Fig.SYSTEM ARCHITECTURE

DOI: 10.17148/IJIREEICE.2022.10579

IV PROBLEM DEFINITION AND DISCUSSION:

Online social networks enable and encourage third party applications (apps) to enhance the user experience on these platforms. Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing games or listening to songs. For example, Face book provides developers an API that facilitates app integration into the Face book user experience. There are 500K apps available on Face book and on average, 20 M apps are installed every day Furthermore, many apps have acquired and maintain a large user base. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Face book leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app: (a) The app can reach large numbers of users and their friends to spread spam, (b) The app can obtain users' personal information such as email address, hometown, and gender, and (c) The app can "re-produce" by making other malicious apps popular. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Face book every day. And additional feature we added into this project Image hotspots. It can be useful for creating info graphics fast and simple. Use any image and enrich it with points of interest and in-depth information about the details depicted. The user is activated by interacting with the image. When the user clicks inside the image the browser will append the X and Y coordinates (relative to the upper-left corner of the image) to the anchor URL as a query string and will access the resulting URL. Users create different gestures on any image of user choice and use those gestures as user password. The gesture can be any combination of circles, pixels, and taps. And additional feature we added into this project Image hotspots. It can be useful for creating info graphics fast and simple. Use any image and enrich it with points of interest and in-depth information about the details depicted. The user is activated by interacting with the image. When the user clicks inside the image the browser will append the X and Y coordinates (relative to the upper-left corner of the image) to the anchor URL as a query string and will access the resulting URL. Users create different gestures on any image of user choice and use those gestures as user password. The gesture can be any combination of circles, pixels, and taps. Pixel is a sample of an original image; more samples typically provide more accurate representations of the original. The intensity of each pixel is variable. In color image systems, a color is typically represented by three or four component intensities such as red, green, and blue, or cyan, magenta, yellow, and black. The term pixel is used to refer to a single scalar element of a multi-component representation. We identify two directions for our future research. One is to further improve the user comments quality by considering more local factors. The other is to explore the effectiveness of the segmentation-based representation for tasks like, search, hash tag recommendation, etc.

V CONCLUSION

In this project, we present the Run length algorithm which segments post into meaningful phrases called segments using both global and local context. Through our algorithm, we demonstrate that local linguistic features are more reliable than term-dependency in guiding the segmentation process. This finding opens opportunities for tools developed for formal text to be applied to tweets which are believed to be much noisier than formal text. Image hotspot is a list of coordinates relating to a specific image, created in order to hyperlink areas of the image to different destinations (as opposed to a normal image link, in which the entire area of the image links to a single destination). For example, a map of the world may have each country hyperlinked to further information about that country. The intention of an image map is to provide an easy way of linking various parts of an image without dividing the image into separate image files.

REFERENCES

1.A. Esfahani, G. Mantas, J. Ribeiro, J. Bastos, S. Mumtaz, M. A. Violas,A. M. D. O. Duarte, and J. Rodriguez, ‘‘An efficient web authentication mechanism preventing man-in-the-middle attacks in industry4.0 supply chain,’’ IEEE Access, vol. 7, pp. 58981–58989,2019,doi-10.1109/access.2019.2914454.

2.M. Trnka, T. Cerny, and N. Stickney, ‘‘Survey of authentication and authorization for the Internet of Things,’’ Secur. Commun. Netw., vol. 2018,pp. 1–17, Jun. 2018, doi: 10.1155/2018/4351603.

3.K. A. Rahman, D. Neupane, A. Zaiter, and M. S. Hossain, ‘‘Web user authentication using chosen word keystroke dynamics,’’ in Proc. 18th IEEE Int.Conf. Mach. Learn. Appl. (ICMLA), Boca Raton, FL, USA, Dec. 2019,pp. 1130–1135, doi: 10.1109/ICMLA.2019.00188.

4. Luke Welling & Laura Thompson ,"PHP & MySQL Web Development – by Luke Welling & Laura Thompson" , Developers Library , 4th edition , 2015.

5. Robin Nixon," Learning PHP, MySQL, JavaScript, and CSS: A Step-by-Step Guide to Creating Dynamic Websites " ,O'Reilly, 2nd edition , 2000.

6.Davey Shafik , "PHP Master (Paperback)" (Goodreads Author) published 2011.