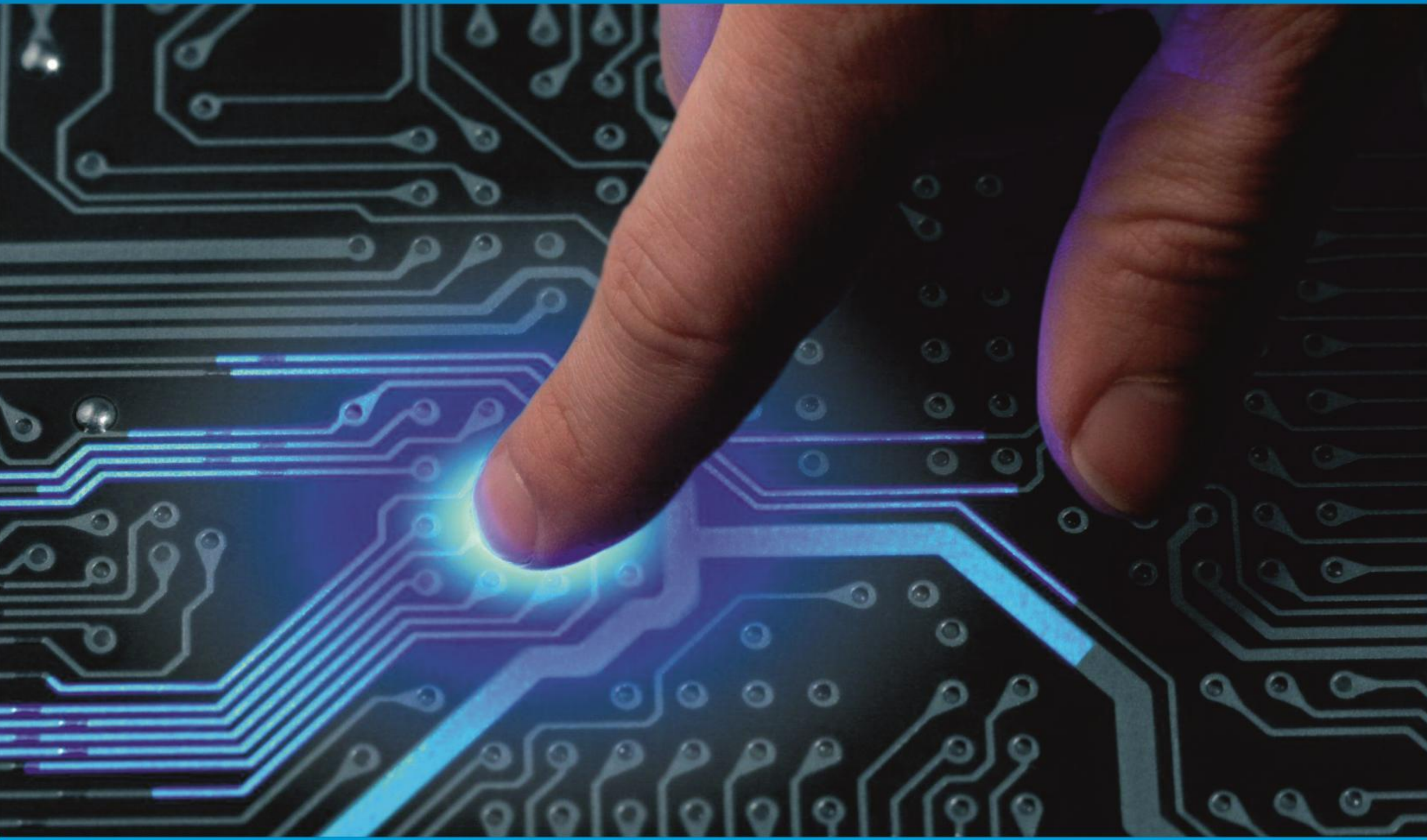
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006104 |

Image Based Authentication Using Zero Knowledge Protocol

Sasikala M[1], Kokila R[2], Archana V[3], Jechiga K[4]

Assistant Professor, Department of Computer Science and Engineering, Dhirajlal Gandhi College ofTechnology, Salem, TamilNadu, India[1]

Student, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, TamilNadu, India[2,3,4]

ABSTRACT*:* One of the most critical concerns in information security today is user authentication. There is a great security when using the text-based strong password schemes but often remembering those good passwords is very hard and users writing them down on a piece of paper or saving inside the smart phone. There is an alternative solution to the text-based authentication which is the Graphical User Authentication (GUA), or simply image-based Password based on the fact that humans tend to memorize images better. This type of approach allows users to create and remember passwords easily. However, one big issue that is plaguing GUA is shoulder surfing attack that can capture the users mouse clicks and eavesdropping. A new algorithm that using zero-knowledge protocol as the solution to be solving the eavesdropping and shoulder surfing attack to provide better system security. In zero-knowledge protocol, users prove that they know the graphical password without sending it. In other words, the user does not send the password to the verifier or reveal it to the people nearby. Hackers who try to eavesdrop the password will be failed since the password is not sent over the insecure channel such as Internet nor reveal. Therefore, it is a secured approach to prevent interception by unwanted parties or adversary. The result that is going to be yielded in this project is a secured authentication approach which is user-friendly.

KEYWORDS*:* Authentication, Image password, Graphical user authentication.

I. INTRODUCTION

The most critical concerns in information security today is user authentication. There is a great security when using the text-based strong password schemes but often remembering those good passwords is very hard and users writing them down on a piece of paper or saving inside the mart phone. There is an alternative solution to the text-based authentication which is the Graphical User Authentication (GUA), or simply image-based Password based on the fact that humans tend to memorize images better. This type of approach allows users to create and remember passwords easily. However, one big issue that is plaguing GUA is shoulder surfing attack that can capture the users mouse clicks and eavesdropping. A new algorithm that using zero-knowledge protocol as the solution to be solving the eavesdropping and shoulder surfing attack to provide better system security. In zero-knowledge protocol, users prove that they know the graphical password without sending it.

In other words, the user does not send the password to the verifier or reveal it to the people nearby. Hackers who try to eavesdrop the password will be failed since the password is not sent over the insecure channel such as Internet nor reveal. Therefore, it is a secured approach to prevent interception by unwanted parties or adversary. The result that is going to be yielded in this is a secured authentication approach which is user-friendly. One other most important aspect in information security is to understand when creating or improving the website's login procedure or known as user authentication. The concept that is useful to secure or authenticate the system is the simple text-based passwords. But it is not secure enough and a burden on the user to remember. There is an alternative solution to these which is Graphical User Authentication (GUA) or imaged-based authentication. This is because humans are good at recognizing images rather than remembering password.

A.SCOPE OF PROJECT

The main objective of this project is to secure a file using Image based passwords.In this We have used encryption and decryption technique for hiding files under a image. By using this technique we can hide our important files.This encrypted key will be strored in a database and it can be used for decryption.We can decrypt our files using that key and find our file path.Its a way of secured authentication and it is user friendly.

B.PROJECT DESCRPTION

Our project is hiding our files using secured authentication .Insome authentication systems, apart from the above-mentioned factors, locations as well as social factors are also used for establishing identity. If only one factor is used for establishing the identity of the user we call that as one factor authentication. If two factors are used for establishing identity than we call that as two factor authentication. A classical example of two factor authentication is the use of credit or debit card and a PIN at the ATM machine. Here we use knowledge factor (PIN) and ownership factor (credit or debit card). In this paper, we describe two level authentication system using knowledge factors. First level is character based i.e username and password and second level is image based.Now whenever user tries to log in, user needs to provide the username password and pass images. Pass images need not be in the same sequence as selected during registration phase. Pass images are randomly distributed on the login rounds. Every round may have all, some or none of the pass images. At least one round need not have pass images to counter intersection attack

II. EXISTING SYSTEM

Computer security is the protection of information systems from theft of damage to the hardware, the software, and to the information on them. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data, and code injection. To achieve this, many techniques were introduced and can be categorized as encipherments, routing protocols, digital signature, data integrity and authentication. Authentication can be categorized into two types which is message authentication and entity authentication. Message authentication is the process to authenticate and verify the message to be sent by the sender and not modified or forged by attacker. While entity authentication is the process of identifying a party to the other party where a party can refer to a user, a process, or a system. User authentication system is the most common entity authentication system implemented and used.In recent years, the inadequacies of the traditional text-based password have been clearly demonstrated. The users of password often aren’t much aware of the security. They habitually use similar words as their password and make it guessable. They need to use alphanumeric uppercase, lowercase to set a strong password which is difficult for the users to remember . Sometimes it leads to brute force attack. The password which h is typed using keyboard or mouse can easily identified using key stroke, mouse movement and shoulder movement. Iris Recognition and retinal scan needs additional hardware support and are very expensive. Fingerprint and Hand geometry needs scanner, and these techniques are futile for dirtiness, injury, arthritis rheumatics and roughness. In the Facial recognition the accuracy is low, and it needs camera as additional device. While considering the signature recognition, we need optical pen and touch panel. The accuracy is very less for signature recognition since the signatures are changeable and easy signature is hackable. In case of the voice recognition system, it needs additional devices but the accuracy is medium. It creates problem because voice is changeable due to age, cold, noise, etc. Other than these disadvantages the biometric passwords create threats as follows: If the computer with the biometric information is connected to the web, the data may be easily retrieved. The biometric information copy can also be fabricated. It is more expensive hence it is not economically an advantageous technology. Hence the social acceptance of these techniques are medium-low. The solutions for these problems are to set images as password which is easy to remember and less vulnerable to password attacks. But currently the system that uses images for authentication is also not well premeditated.

Disadvantages:

- Require much more storage space than text-based passwords.
- Password registration and log-in process take too long.
- Shoulder Surfing: As the name implies, shoulder surfing is watching over people's shoulders as they process information.

A.Proposed System

Biometric authentication is, over time, becoming an indispensable complementary component to traditional authentication methods that use passwords and tokens. As a result, the research interest in the protection techniques for the biometric template has also grown considerably. We present a light-weight AI-based biometric authentication that operates based on the binary representation of a biometric instance. In details, a binary classifier will be trained using the binary strings that represent the intraclass and interclass biometric subjects. The Support Vector Machine and Multi-layer Perceptron Neural Network are chosen as the classifier to evaluate the fingerprint-based and iris-based authentication capability. Afterward, the authenticated biometric string is fed to a hash function to produce a hash value, which is to be used in a Zero-Knowledge-Proof Protocol for the purpose of privacy preservation. In order to improve the recognition of the classifier, we devise a simple yet efficient strategy to enhance the discriminativeness of the binary strings and name it the Composite Features Retrieval. We use images along with the password to overcome the problem which arises because of sharing and selection of weak passwords. Hence the system aims to achieve following: Authentication should not be based on precise recall of password. Make it difficult to share or write passwords. Provide good user experience. Also it’s a proven fact that human user recognizes images faster as compared to recall of words . Standing shows that people can recognize images in spite of distracters and can retain over a period of time.In graphical authentication there are various techniques to secure your password. Here we are proposing a new algorithm of authentication using images. We used a grid based approach to authenticate by using image as a reference. At the time of registration, user will upload his/her image or set of images along with all details; then user selected image will appear on the page with transparent grid layer on it.

Advantages

- Using Image Retrieval user can choose their own choice of image as pass images and can increase password space.
- We have also discussed their effect on usability and security, which provides resistance to shoulder surfing attack.
- Adds one more layer of security to the existing system and hence makes the system more secure.

III. ENCRYPTION AND DECRYPTION

Select the file that need to be encrypted.The file has been encrypted under the image we have selected.The key will be generated after the file has been encrypted.Using that key we will decrypt our file and find our file path.There are two types of cryptographic schemes in use today: private key or secret key (also known as symmetric) cryptography and public key (also known as asymmetric) cryptography. Symmetric key cryptography uses the same key for encryption and decryption. Another type of encryption method, asymmetric or public key cryptography uses different keys to encrypt and decrypt. On one hand, asymmetric key cryptography requires more computation resources than symmetric key cryptography does, on the other hand, symmetric key cryptography is difficult for key deployment and management. Though most framework use one type of cryptography, there still exist some schemes that use both asymmetric-key and symmetric-key cryptography.

Recognition-Based Graphical Password

Recognition based graphical password scheme creates a platform for the user to select pictures from a variety of images provided, during authentication the user is asked to recognize the previously selected images to gain access hence, the name recognition based graphical scheme. Another recognition-based graphical password system is Déjà vuproposed by Dhamija and Perrig, which authenticates the users by choosing pictures among the set of fake pictures. These pictures are presented in random manner.Each picture is derived from an initial seed and no need to store the pictures pixel by pixel so only the seeds need to be stored in the server.Therefore, an authentication server does not need to store the whole picture, it simply needs to store the initial seed. In order to login, users should remember the selected portfolios images from a decoy image collection. In the test system, a panel including 25pictures ispresented; out of these, 5 images are included in user‟s the portfolio. The users should remember all images of their portfolio but only one panel is displayed. When “Randomart" images are employed, the users have difficulty disclose their password to others through image portrayal or jotting it. It is claimed that a set of 10,000 fixed images is sufficient; nevertheless, eye-catching images should be selected accurately so that users have higher chances of picking similar probable image. A study reported that this authentication technique was successfully used.The security of the system is very high. Graphical password schemes provide a way of making more human-friendly passwords. Dictionary attacks and brute force search are infeasible.The graphical password is possibly easier to remember and more secure compared to traditional alphanumeric password as they make use of humans‟ capability of memorizing and recalling images better.

IV. CONCLUSIONS

Nowadays, graphical user authentication is one of the important topics in information technology. Graphical authentication has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. However, one big issue that is plaguing graphical user authentication is shoulder surfing attack that can capture user mouse click and eavesdropping. Unlike tradition text-based password which can be masked right after user input, image based password lack of effective way to mask the input of user when login. This paper had discussed an approach to combine recognition method in graphical user authentication and Zero-knowledge protocol to mask the users input when attempt to login. It increased the resistance of this graphical user authentication system to shoulder surfing attack used by hackers. The application of this algorithm had helped easing business organizations and casual operations in considering security mechanisms used to ensure authentication of users. The system implemented project can indeed provide a very secure graphical user authentication function. To increases security of this system, system should reserve and choose a series of image for user to select as password instead of let users to upload their own image as it is hard to standardize image upload by users. This can make users' password harder to be recognize by hacker who attempt to guess users' password. Research on simplifying Zero knowledge protocol can help reducing the time taken and amount of system resources used in authenticating user.

REFERENCES

[1]. Network Behrouz A. Forouzan, Cryptography and Security, 2008. Greg E. Blonder, Graphical Password U.S. Patent No. 5559961, 1996.
[2]. A.H. Lashkari, F.T., Graphical User Authentication (GUA).2010: Lambert Academic Publisher.
[3]. Louis C. Guillou, Jean-Jacque Quisquater, C.G.Guethen(Ed): Advances in Cryptology – EUROCRYPT' 88, LNCS 330.pp. 123- 128, 1988.
[4]. Arash Habibi Lashkari, Maslin Masrom, Azizah Abdul Manaf, A Secure Recognition Based Graphical Password by Watermarking, 2011 11th IEEE International Conference on Computer and Information Technology.
[5]. R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years,"ACMComput. Surveys, vol. 44, no. 4, 2012.
[6]. H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp.760–767.
[7]. Indian Journal of Science and Technology, Vol 9(39), DOI:10.17485/ijst/2016/v9i39/86878, October 2016 by Ahmad M. Odat1 and Mohammed A. Otair2.
[8]. Muhammad Daniel Hafiz, Abdul Hanan Abdullah, NorafidaIthnin, HazinahK.Mammi; "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique"; IEEE Explore, 2008.
[9]. Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy;" Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice", Symposium On Usable Privacy Pittsburgh, PA, USA, 2005.
[10]. Arash Habibi Lashkari, GPIP: A new Graphical Password Based on Image Portions.2014.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details