International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST229343

Secure Data Access using Steganography and Image Based Password

Prof. P. S. Gayke[1], Shraddha Thorat[2], Gayatri Nagarkar[3], Priyanka Kusalkar[4], Priyanka Waditake[5]
Assistant Professor[1], [2,3,4,5] Student
Department of Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar
Savitribai Phule Pune University, Pune, Maharashtra, India

Article Info
Volume 9, Issue 3
Page Number : 193-198

Publication Issue
May-June-2022

Article History
Accepted : 10 May 2022
Published : 20 May 2022

ABSTRACT

Technology has developed to a very great extent, and the use of smart systems has introduced an increasing threat to data security and privacy. Most of the applications are built-in unsecured operating systems, and so there is a growing threat to information cloning, forging tampering counterfeiting, etc. This will lead to an un-compensatory loss for end-users particularly in banking applications and personal data in social media. The shoulder surfing attack in an assault that can be achieved with the aid of the adversary to accumulate the individual's password by way of searching over the client's shoulder as he enters his password. As conventional password schemes are vulnerable to Shoulder Surfing, Steganography and Cryptography proposed three shoulder surfing resistant graphical password schemes. However, most of the current graphical password schemes is liable to shoulder-browsing a recounted hazard wherein an attacker can seize a password by means of way of direct statement or by recording the authentication consultation. Because of the visual interface, shoulder-browsing becomes an exacerbated problem in graphical passwords. A graphical password is easier than a textual content-based password for the majority to undergo in thoughts. Suppose an eight-man or woman password is critical to benefit access into a specific computer network. Sturdy passwords may be produced which might be proof against guessing, dictionary assault. Key-loggers, shoulder surfing and social engineering. Graphical passwords have been utilized in authentication for mobile phones, ATM machines, E-transactions.

Keywords: Shoulder Surfing, Steganography and Cryptography, Image Processing, Classification, Shoulder Surfing, Training Images, OTP, Secret Bit, Keylogging

I. INTRODUCTION

Recently, Biometric-based authentication techniques are growing frequently successful compared to knowledge-based methods such as identification cards, passwords, etc.[4]. Digital watermarking is the necessary method required to resolve this problem [5]. The purpose of steganography is to hide the data, also excluding the suspicion in having protected information [6]. In medical images, Region of interest (ROI) lossless watermarking and reversible watermarking are two technologies employed to protect the authentication and integrity [8].

For economic data such as money and interest rates, the assurance of sensitive information becomes more and more important. Several techniques have been improved to increase security and data privacy. However, this paper mainly focuses on increasing the data privacy, security, and ownership of sub-optimal multimedia applications. Threats in opposition to electronic and financial offerings may be classified into two foremost instructions: credential stealing and channel breaking assaults. Credentials consisting of customer's identifiers, passwords, and keys may be stolen by an attacker when they're poorly managed. As an example, a poorly controlled personal pc (computer) inflamed with malicious software (malware) is a smooth goal for credential attackers. On the other hand, channel breaking attacks which permit for eavesdropping on conversation between customers and a monetary institution are another form of exploitation. At the same time as classical channel breaking assaults can be avoided by means of the proper utilization of a protection channel inclusive of IPSec and at ease sockets layer (SSL), recent channel breaking attacks are extra challenging. Indeed, keylogging assaults or people who make use of session hijacking, phishing and pharming, and visible fraudulence cannot be addressed by using simply enabling Quantum Cryptography. The shoulder browsing attack in an assault that can be achieved with the aid of the adversary to accumulate the individual's password by way of searching over the clients shoulder as he enters his password. As conventional password schemes are vulnerable to shoulder surfing, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes. However, most of the current graphical password schemes is liable to shoulder-browsing a recounted hazard wherein an attacker can seize a password by means of way of direct statement or by recording the authentication consultation. Because of the visual interface, shoulder-browsing becomes an exacerbated problem in graphical passwords. A graphical password is easier than a textual content-based password for the majority to undergo in thoughts. Suppose an eight-man or woman password is critical to benefit access into a specific computer network. Sturdy passwords may be produced which might be proof against guessing, dictionary assault. Key-loggers, shoulder-surfing and social engineering. Graphical passwords have been utilized in authentication for mobile phones, ATM machines, E-transactions.

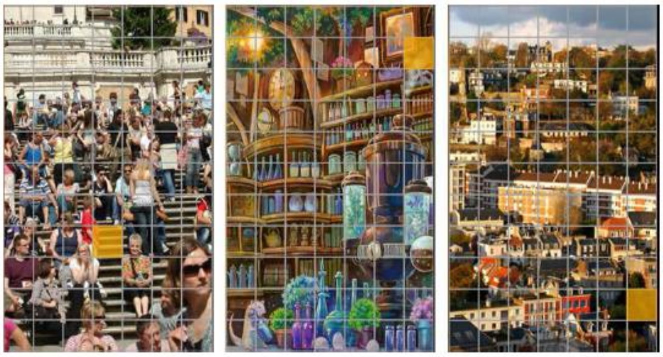

Figure 1: Shoulder Surfing Graphical Password

II. LITERATURE SURVEY

Smart ShraddhaM. GuravLeena S. GawadePrathamey K. RaneNilesh R. Khochare. "Graphical Password Authentication". [1]Graphical password is one of the alternative solutions to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally, cloud is provided with this graphical password authentication.

RachnaDhamija Adrian Perrig. “Deja Vu: A User Study Using Images for Authentication”.[2]Current secure systems suffer because they neglect the importance of human factors in security. We address a fundamental weakness of knowledge-based authentication schemes, which is the human limitation to remember secure passwords. Our approach to improve the security of these systems relies on recognition-based, rather than recall-based authentication. We examine the requirements of a recognition-based authentication system and propose D´ej`a Vu, which authenticates a user through her ability to recognize previously seen images. D´ej`a Vu is more reliable and easier to use than traditional recall-based schemes, which require the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others.

Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memon. “PassPoints: Design and longitudinal evaluation of a graphical password system”.[3] Computer security depends largely on passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password that is long and random. Therefore, they tend to choose short and insecure passwords. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. In this paper we describe PassPoints, a new and more secure graphical password system. We report an empirical study comparing the use of PassPoints to alphanumeric passwords. Participants created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over the course of 6 weeks. The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. However, the graphical users took longer and made more invalid password inputs than the alphanumeric users while practicing their passwords. In the longitudinal trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password.

Sacha Brostoff & M. Angela Sasse. “Are Passfaces More Usable Than Passwords? A Field Trial Investigation”.[4] The proliferation of technology requiring user authentication has increased the number of passwords which users have to remember, creating a significant usability problem. This paper reports a usability comparison between a new mechanism for user authentication - Passfaces – and passwords, with 34 student participants in a 3-month field trial. Fewer login errors were made with Passfaces, even when periods between logins were long. On the computer facilities regularly chosen by participants to log in, Pass-faces took a long time to execute. Participants consequently started their work later when using Pass-faces than when using passwords, and logged into the system less often. The results emphasize the importance of evaluating the usability of security mechanisms in field trials.

Martina Angela Sasse, Sacha Brostoff & Dirk Weirich, “Transforming the ‘Weakest Link’: A Human-

Computer Interaction Approach for Usable and Effective Security"[5]. The security research community has recently recognized that user behavior plays a part in many security failures, and it has become common to refer to users as the "weakest link in the security chain". We argue that simply blaming users will not lead to more effective security systems. Security designers must identify the causes of undesirable user behavior, and address these to design effective security systems. We present examples of how undesirable user behavior with passwords can be caused by failure to recognize the characteristics of human memory, unattainable or conflicting task demands, and lack of support, training and motivation. We conclude that existing Human-Computer Interaction (HCI) knowledge and techniques can be used to prevent or address these problems, and outline a vision of a holistic design approach for usable and effective security.

III. PROBLEM STATEMENT

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks.

Here Password authentication protocol is set at the time of sign-up in the form of secret bit matrix by clicking on the fields of the matrix on the terminal, user can securely login to its account without being attacked.

IV. RELATED WORK

When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to as phishing, shoulder-surfing and is a known risk, of special concern when authenticating in public places. Until recently, the only defense against known attacks was the alertness on the part of the user. Anti-Phishing authentication mechanism assure known attacks resistant authentication to user. It allows user to authenticate by entering password in graphical way at insecure places because user never have to click directly on password icons. Usability testing of this mechanism showed that novice users were able to enter their graphical password accurately and to remember it over time. However, the protection against known attacks comes at the price of longer time to carry out the authentication with the help of Steganography as well as Cryptography.

V. PROPOSED SYSTEM

The Proposed Methodology of the system is as follow which contain some important points such as algorithm etc. To overcome existing attacks we developed a keylogger virtual continuous visual authentication system through which users can easily authenticate to the system without losing information.

Image-based verification using visual cryptography is proposed in [2]. Visual cryptography is used to transform the QR code with encrypted format and shares and both these shares transmitted separately. This methodology was implemented image-based authentication using visual cryptography. Using this method, the user can determine whether the site is safe or unsafe to carry out his transaction. In this system, we prove that this method is more efficient and secured.

VI. SYSTEM ARCHTECTURE

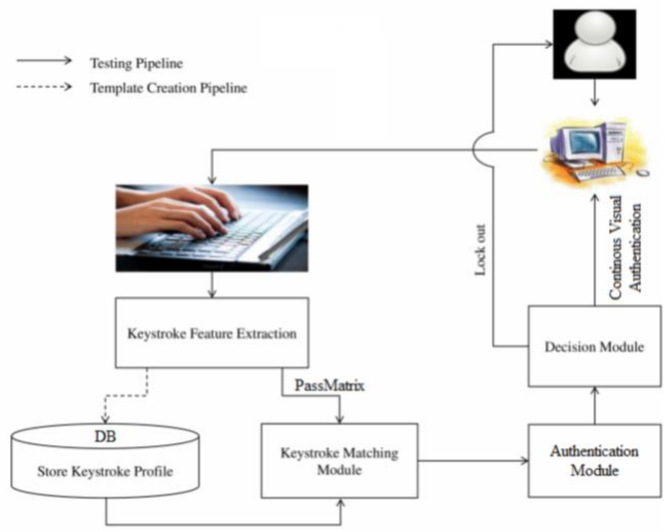
Testing Pipeline
Template Creation Pipeline
Lock out
Continous Visual Authentication
Keystroke Feature Extraction
PassMatrix
DB
Store Keystroke Profile
Keystroke Matching Module
Authentication Module
Decision Module

Fig.1 System Architecture

The architectural design of the system is as follows which contain some important points such as algorithms etc.

1. Two protocols for password-based authentication and one-time pass-word based authentication that uses visualization by technique for increased reality to give both high security and high convenience. Both conventions offer great circumstances in light of visualization both as far as security and convenience.

2. Model utilization as Android applications which demonstrate the convenience of our conventions in true organization settings.

VII. CONCLUSON

In this proposed work we introduce a system that makes use of user-driven visualization to improve the security and user-friendliness of continuous authentication protocols. Protocols utilize simple technologies available in most Smartphone devices. The proposed protocol not only improves the user experience but also resists challenging attacks, such as the keylogger and malware attacks. In this project, we proposed a method for Online Fraud Transaction prevention as well as provide security for confidential data using extended visual cryptography as well as steganography techniques. Using extended visual cryptography we can verify the shares are genuine or not. Therefore, it provides better security in preventing phishing attacks compared to visual cryptography.

VIII. ACKNOWLEGEMENT

I would prefer to give thanks the researchers likewise publishers for creating their resources available. I'm conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

IX. REFERENCES

[1]. A Yahaya Lawal Aliyu, Madihah Mohd Saudi, Ismail Abdullah, A Review and Proof of Concept for Phishing Scam Detection and Response using Apoptosis". (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[2]. Gori Mohamed J, M. Mohammed Mohideen, Mrs. Shahira Banu. N, "E-Mail Phishing – An open threat to everyone". International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014 1 ISSN 2250-3153

[3]. Rana Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches". Future Internet Journal 2020

[4]. David Lacey, Paul Salmon, Patrick Glancy, "Taking the bait: a systems analysis of phishing attacks". International Conference on Applied Human Factors and Ergonomics (AHFE 2015)

[5]. Ike Vayansky and Sathish Kumar, "Phishing – challenges and solutions". Computer Fraud & Security January 2018.

[6]. S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009.

Proceeding of International Conference on, Dec 2009, pp. 1–7.

[7]. S. Gurav, L. Gawade, P. Rane, and N. Khochare, “Graphical password authentication: Cloud securing scheme,” in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[8]. K. Gilhooly, “Biometrics: Getting back to business,” Computerworld, May, vol. 9, 2005. R. Dhamija and A. Perrig, “Deja vu: A user study using images for authentication,” in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[9]. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[10]. A. Paivio, T. Rogers, and P. Smythe, “Why are pictures easier to recall than words?” Psychonomic Science, 1968.

[11]. D. Nelson, U. Reed, and J. Walling, “Picture superiority effect,” Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[12]. A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, “Vip: a visual approach to user authentication,” in Proceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323

Cite this article as :

Prof. P. S. Gayke, Shraddha Thorat, Gayatri Nagarkar, Priyanka Kusalkar, Priyanka Waditake, "Secure Data Access using Steganography and Image Based Password ", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 3, pp. 193-198, May-June 2022. Available at doi : https://doi.org/10.32628/IJSRST229343

Journal URL : https://ijsrst.com/IJSRST229343