Anti Phishing Mechanism for Securing Login Details Using Login Authentication Mechanism

Veer Shreekant[1], Yadav Ashish[2], Suroshe Swapnil[3], Nalawade Suraj[4], Prof. U. Mande[5]

[1,2,3,4] Students and [5]Asst. Prof. of STES' Sinhgad Institute of Technology, Lonavala

Savitribai Phule Pune University, Pune,

Maharashtra, India.

Abstract:—Nowadays many of us do online financial transactions. This transaction must be secure. There are various attacks present behind this. Phishing is one sort of attack. For detecting this attack, various anti-phishing mechanisms are used. Within the phishing process, suppose the cheater sends out thousands of phishing emails with a link to the fake website. Victims click on links in email believing it's legitimate. They enter personal information thereon fake website. Fraudsters collect the stolen data and login into the right website. This is often an overall process of phishing. We propose a replacement scheme for online fraud transaction prevention using extended visual cryptography and QR codes. This scheme uses extended visual cryptography for share generation. A one-time password is employed for phishing website detection. Extended visual cryptography is employed for converting the QR code into two shares. The system provides security for online users and detecting phishing websites. Keylogging or keyboard capturing is that the activity of recording (or logging) the keys struck on a keyboard, normally during a secretive way in order that the individual utilizing the keyboard is unconscious that their activities are being observed. It likewise has exceptionally authentic uses in investigations of human-computer interaction. There are various Keylogging techniques, extending from hardware and software-based methodologies to acoustic examination. Including humans in authentication protocols, while guaranteeing, isn't simple in light of their restricted capacity of calculation and remembrance. We exhibit how careful visualization outlines can improve the safety also because the convenience of authentication. We propose two visual authentication protocols: one may be a one-time-password protocol, and therefore the other may be a password-based authentication protocol. Our approach for genuine arrangement: we could attain an abnormal state of simple use while fulfilling stringent security necessities.

Keywords: OTP, Phishing, QR code, extended visual cryptography, visual authentication protocols, Keylogging, etc.

I. INTRODUCTION

Recently, when a user goes to any site for purchase or any operation, the first step is to authenticate to his account and after that user can perform his task. If the login credentials or confidential information about the user is not secured, the system is not worth using. Various systems are currently available to provide security to a user from various attacks. The first type is to type a password protocol using a keyboard. If the attacker is present on a system, the attacker tracks the keys pressed and knows the password entered (Keylogging attack). The second type is graphical images if the attacker is behind the user then the attacker knows the images selected (Shoulder surfing).

In this kind of cyber attack, people will easily see the password of some other users when they are in a public area if the password is not that tough. So it will be hazardous if the password is getting hack by any

unauthorized person. In the existing system, we are using images for authentication but it was easy for the attacker to remember those images. To overcome these kinds of attacks we proposed a Keylogging resistant continuous visual authentication protocol system. Whenever users authenticate to the system, the virtual keyboard will display on the terminal and use that keyboard to enter the password. The keys on that keyboard shuffle every time. The user needs to feed his information into the database. Then, the system will generate a 2D dynamic Quick Residual Code. This 2D dynamic Quick Residual Code will be used whenever information about a particular user is needed.

II. LITERATURE SURVEY

- A. Yahaya Lawal Aliyu, Madihah Mohd Saudi, Ismail Abdullah, [1] Phishing scam is a well-known fraudulent activity in which victims are tricked to reveal their confidential information especially those related to financial information. There are various phishing schemes such as deceptive phishing, malware based phishing, DNS-based phishing and many more. Therefore in this paper, a systematic review analysis on existing works related with the phishing detection and response techniques together with apoptosis have been further investigated and evaluated. Furthermore, one case study to show the proof of concept how the phishing works is also discussed in this paper. This paper also discusses the challenges and the potential research for future work related with the integration of phishing detection model and response with apoptosis. This research paper also can be used as a reference and guidance for further study on phishing detection and response.
- Gori Mohamed J, M. Mohammed Mohideen, Mrs. Shahira Banu. N. [2] we cannot imagine a day without a computer especially without Internet. E-Mail is one of the primary ways through which we communicate. We not only use it every day for official communication but also to be in touch with our friends and relatives. As E-Mail plays a vital role in communication globally for communication and sharing of data as well. The security issues also have increased. The major problem or the attack on E-Mail by the hackers nowadays is known as E-Mail Phishing. It is the right time to secure the data communicated over mail even on trusted network. Cyber criminals craft these emails to look convincing, sending them out to literally millions of people around the world. The criminals do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know the more emails they send out, the more people they may be able to fool. In this paper we are analyzing the various ways in which the Phishing is achieved, the possible solutions and the awareness along with some tips to be away from a victim of Phishing attacks are discussed.
- Rana Alabdan, [3] Phishing attacks, which have existed for several decades and continue to be a major problem today, constitute a severe threat in the cyber world. Attackers are adopting multiple new and creative methods through which to conduct phishing attacks, which are growing rapidly. Therefore, there is a need to conduct a comprehensive review of past and current phishing approaches. In this paper, a review of the approaches used during phishing attacks is presented. This paper comprises a literature review, followed by a comprehensive examination of the characteristics of the existing classic, modern, and cutting-edge phishing attack techniques. The aims of this paper are to build awareness of phishing techniques, educate individuals about these attacks, and encourage the use of phishing prevention techniques, in addition to encouraging discourse among the professional community about this topic.

- David Lacey, Paul Salmon, Patrick Glancy, [4] This paper is a response to this key knowledge gap, analyzing the tasks and mapping the social interactions of a phishing attack and the associated response. To achieve this, the research team adopted a multi-method approach in examining the underlying functions and interactions involved in a phishing attack and its response by deliberately 'taking the phishing bait', interviewing a sample of individuals that had unwittingly responded to phishing attacks, and engaging with organizations that took response measures to such events. This multi-actor engagement provided critical observations and content about the victim experience and interactions with those responsible for the attacks. The research is highly novel in its application of Work Domain Analysis (WDA) to gain an understanding of the functional structure of phishing attacks and the online transactional environment they target as a socio-technical system. By examining the functional properties of interactions within the research context, the paper provides a unique perspective of phishing and the inter-linkages and dependencies across multiple levels of abstraction from the initial 'baiting' to the achievement of overall system objectives by cybercriminals. The findings provide opportunities to enhance phishing prevention and detection methodologies, improve individual resilience to such attacks, and pave the way for future efforts in applying socio-technical systems methods to the cybercrime environment.
- Ike Vayansky and Sathish Kumar,[5] Phishing is a major threat to all Internet users and is difficult to trace or defend against since it does not present itself as obviously malicious in nature. In today's society, everything is put online and the safety of personal credentials is at risk. Phishing can be seen as one of the oldest and easiest ways of stealing information from people and it is used for obtaining a wide range of personal details. It also has a fairly simple approach – send an email, email sends victim to a site, and site steals information.

III. PROBLEM STATEMENT

In this system we design and develop an Anti Phishing Mechanism for Securing front end security system in which user information is stored in the database and Quick Response code is used to retrieve that information. The password authentication protocol is sent to the user's mail in the form of a matrix (virtual keypad) and by clicking on the fields of the matrix on the terminal, the user can securely log in 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 Quantum 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:-

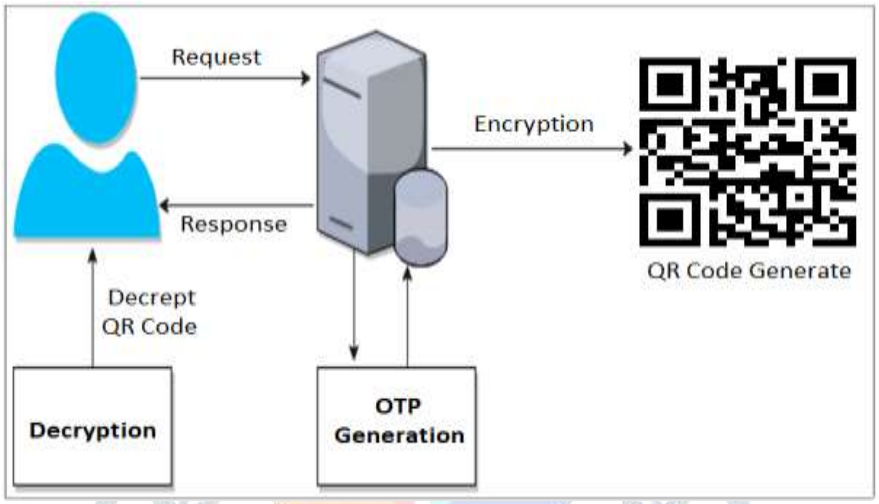

Fig.1 System Architecture

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 and QR code 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.

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.

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