IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207173 |

Transaction and login Authentication Using Visual Cryptography

Naveen R, Dr H K Madhu

Master of Computer Applications, Bangalore Institute of Technology, Bengaluru, India

Master of Computer Applications, Bangalore Institute of Technology, Bengaluru, India

ABSTRACT: The main aim of banking software is to provide efficient and secure solutions for managing various banking operations and services. The software is designed to streamline and automate a wide range of financial processes, both for the bank and its customers. Some of the key objectives and purposes of banking software include:

Transaction Processing: The software facilitates the processing of various types of transactions, including deposits, withdrawals, fund transfers, bill payments, and other financial activities in a fast and accurate manner.

Security: Security is a paramount concern in banking software. The aim is to safeguard sensitive customer information, prevent fraudulent activities, and ensure secure communication between the bank and its customers.With the rise of online databases being hacked, it's challenging to trust the information available on websites.

To tackle the authentication problem, a new method is being proposed, which involves using image processing and steganography. In this approach, the bank generates a certain number of shares based on their chosen plan. When a customer is onboarded, two shares are created: one for the bank maember to keep and the other stored in the bank's database.The customer must present his or her portion at each transaction. The original image is obtained by fusing this share with the baseline share kept in the database. The hidden password is then revealed after this image has undergone a decoding procedure, aiding in client authentication and deciding whether the transaction will be approved or refused.

I. INTRODUCTION

Using steganography for authentication in a banking software login page is an interesting concept, but it's important to consider the security implications and practicality of such an approach. Here's an outline of how steganography could be used for authentication in a banking software login page:

Account Registration: During the account registration process, the user would provide their account details, including a secure password, to the bank's system. The system could then generate a steganographic image containing some critical account information and the user's password embedded in it.

Login Process: When the user attempts to log in, they would be asked to upload an image (e.g., a profile picture) along with their username and password. The system would then extract the embedded information from the uploaded image, including the user's password.

Authentication: The extracted password would be compared to the password stored in the bank's database during the account registration process.If the passwords match, the user is granted access to their account.

Phishing is recognised as a significant security issue in these types of attacks, and new inventive ideas are developing with it every second, therefore preventive procedures should also be very effective. Thus, ”Transaction sand login Authentication Using visual cryptography” is a new technique that can be utilised asa secure defence against phishing

II. LITERATURE SURVEY

Design and development of a Viusal Cryptography Based Anti-phishing Framework When registering for the secure website, the user is requested for a key String (password). An image captcha is created by concatenating this string with a randomly generated string in the server. Two shares of the image captcha are created, one of which is maintained on the bank member computer and the other of which is retained on the server.

.The research highlights the importance of creating representative datasets for training and evaluating the content-based anti-phishing approach. Datasets should include a diverse range of phishing and legitimate samples, covering

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207173 |

various attack vectors and scenarios. Evaluation metrics, such as precision, recall, F1-score, and receiver operating characteristic (ROC) curves, are used to access one of the performance of the proposed approach.[1]

One may determine whether a website is genuine/secure or a phishing website using the login credentials and Image Captcha created via Stacking Two Shares, as well as whether the individual visiting it is human or computer. Phishing Classification techniques the systematic literature review

The paper concludes by summarizing the key contributions of ACRM as an effective anti-phishing technique. It highlights the importance of continuous research and development in combating evolving phishing attacks and emphasizes the need for collaborative efforts in improving cybersecurity. Phishing attacks are a significant threat to cybersecurity, aimed at deceiving users and stealing sensitive information. Traditional anti-phishing methods have limitations and areoften ineffective in detecting and preventing sophisticated phishing attacks. The paper proposes an innovative approach called the Automated Challenge Response Method (ACRM)to combat phishing attacks effectively.[2].

In this study, the paper concludes by highlighting the importance of DNS-based anti-phishing approaches in combating evolving phishing threats. It emphasizes the need for continued research and collaboration to stay ahead of attackers and protect users from falling victim to phishing attacks. Phishing attacks continue to pose a significant threat to internet users, requiring innovative techniques for detection and prevention. This research paper proposes a DNS-based anti-phishing approach to enhance security and protect users from falling victim to phishing attacks. The proposed approach emphasizes real-time monitoring of DNS requests and responses to detect and prevent phishing attacks promptly. Anomaly detection algorithms and heuristics areemployed to identify suspicious patterns or inconsistencies in DNS traffic. The paper discusses the application of machine learning algorithms to analyze DNS data and identify potential phishing domains. The research paper presents an evaluation of the proposed visual cryptography scheme for general access structures. Performance metrics, such as image quality, reconstruction accuracy, and computational overhead, are considered to assess the effectiveness of the approach. Supervised learning models can be trained on labeled datasets to classify domains as legitimate or malicious based on various features. The paper emphasizes the importance of collaboration between organizations to share information about identified phishing domains. A collaborative DNS threat intelligence network can enhance the detection and prevention capabilities by leveraging a larger database of known malicious domains.[3].

In this study, the paper concludes by highlighting the effectiveness of a content-based anti-phishing approach that combines textual and visual content analysis. It emphasizes the importance of ongoing research to adapt to evolving phishing techniques and the significance of user education

in combating phishing attacks. Phishing attacks exploitboth textual and visual elements to deceive users and steal sensitive information. This research paper proposes a content- based anti-phishing approach that analyzes both textual and visual characteristics to detect and prevent phishing attacks effectively. The research emphasizes the importance of analyzing visual content, including logos, images, and website layouts, to detect phishing attempts. Image processing and computer techniques are employed to identify manipulated or counterfeit logos, inconsistent branding, orsuspicious website structures.[4].

In the study, the paper concludes by summarizing the contributions and findings related to visual cryptography for general access structures. It highlights the potential of this cryptographic technique in addressing security and privacy requirements in various applications and suggests avenues for future research and development. Visual cryptography is a cryptographic technique that enables secure sharing of secret information among multiple participants without requiring complex computations. This research paper focuses on visual cryptography for general access structures, where secret information is distributed to a specific group of participants based on a predefined access structure. The research paper explains the encoding process, where the secret imageis divided into shares using specific visual cryptography algorithms. The decoding process involves combining the shares held by the participants based on the access structureto reconstruct the secret image.[5].

In this study, the paper concludes by summarizing thekey contributions of ACRM as an effective anti-phishing technique. The authors acknowledge the importance of considering usability and user experience aspects while implementing ACRM. Balancing security and user convenience is crucial to ensure that the challenge-

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207173 |

response process is not overly burdensome for legitimate users It highlights the importance of continuous research and development in combating evolving phishing attacks and emphasizes the need for collaborative efforts in improving cybersecurity. Phishing attacks are a significant threat to cybersecurity, aimed at deceiving users and stealing sensitive information. Traditional anti-phishing methods have limitations and are often ineffective in detecting andpreventing sophisticated phishing attacks. The research paper proposes an innovative approach called the Automated Challenge Response Method (ACRM) to combat phishing attacks effectively.[6].

In this study, the paper concludes by summarizing the contributions and findings of the phishing detection system for e-banking. It emphasizes the importance of utilizing intelligent techniques, particularly fuzzy data mining, to enhance the security of e-banking platforms and protect customers from phishing attacks. The research proposes an intellgent phishing detection system that leverages fuzzy data mining techniques. Fuzzy data mining allows for the analysis of imprecise and uncertain data, which is particularly relevant in the context of phishing detection. The paper also suggests future research directions, such as the integration of real-time data streams and continuous monitoring for improved phishing detection capabilities. Phishing attacks targeting ebanking platforms pose a significant threat to the security of financial transactions and customer data. This research paper presents a novel approach that combines intelligent techniques, including fuzzy data mining, to develop an effective phishing detection system for e-banking.[7].

III.METHODOLOGY

The foremost applications are as it were as secure as their underlying framework. Since the plan and innovation of middleware has moved forward relentlessly, their location is a difficult issue. As a result, determining if a computer connected to the inter may be regarded as reliable and secure or not is next to impossible. Additionally, phishing schemes are becoming a problem for online account management and online customers. How to handle applications that demand a security is the topic at hand. Phishing is a sort of online identity theft that refers to the theft of sensitive[6] information from victims, such as their credit card numbers and online banking passwords. Since these attacks are becoming more frequent and sophisticated, phishing techniques have received extensive press coverage.

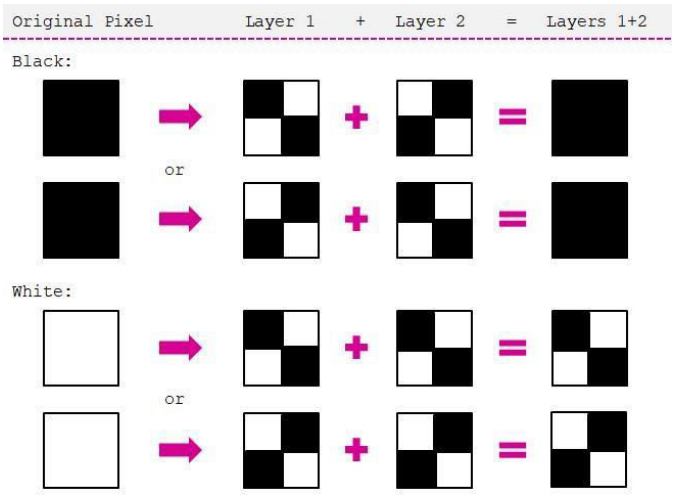
Not secure,Phishers can obtain private information about individuals, including passwords and credit card numbers. Fake websites that look like the actual website The method of heuristic-based anti-phishing, with a tall likelihood of untrue and fizzled caution, and it is simple for the aggressor to utilize specialized implies to dodge the heuristic characteristics discovery.

To solve the authentication problem, we proposed an algorithm based on processing and developed steganography. This is good for important companies, so only authorized people can access the Internet from anywhere in the world. This system offers them an effective solution to prevent attacks. Within the net keeping money framework, the secret word of client may be hacked and abused. In this way security is still achallenge in these applications. Here we propose a method secure the client data and to anticipate the conceivablefraud of watchword hacking. Visual cryptography couldbe a cryptographic procedure that permits for the secure transmission of mystery data through visual means such as pictures or designs. The fundamental thought behind visual cryptography is to partition a mystery picture into different offers or parts that are aimless independently, but when combined together, they uncover the mystery message

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207173 |



IV. SYSTEM ARCHITECTURE

Designing the system architecture for the "Transaction and login Authentication Using visual cryptography" project involves identifying the main components and their interactions to achieve the intended goals of enhancing security in online transactions. Below is a high-level overview of the system architecture:

1. User Interface (UI):
This is the front-end component that interacts with users. It provides the interface for users to input sensitive data and initiate transactions (e.g., online banking transactions, e-commerce purchases). The UI also handles the display of steganographically encoded images to users to verify the authenticity of the website.

2. Application Layer:
The application layer is responsible for processing user requests, managing user sessions, and handling the business logic of the system.It integrates with other components for authentication, steganography encoding, decoding, and validation.

3. Authentication Module: This module is responsible for user authentication and ensuring that only authorized users can access sensitive functionality.

4. Steganography Encoding Module :The steganography encoding module takes textual data and encodes it into images using steganography techniques.It ensures that the encoded images appear normal and do not raise suspicion to the users.

5. Steganography Decoding Module :The decoding module is responsible for extracting the hidden information from the steganographically encoded images.It processes the images to reveal the original text, which is used to verify the website's identity and transaction details.

6.Image Process Module The image processing module is responsible for manipulating images, dividing them into shares, and merging the shares during the decoding process.It implements the necessary algorithms for image splitting and combining required for visual cryptography.

V. RESULT AND DISCUSSION

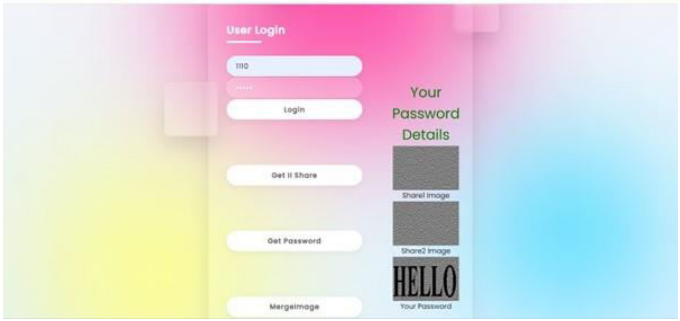
Phishing attacks are so prevalent right now because they may target anyone and collect and keep sensitive data about the users. The attackers, who were indirectly involved in the planning of the phishing attack, use this information. Our "Anti-phishing system based on Visual Cryptography" can quickly identify fraudulent websites as

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207173 |

well as actual customers. Three layers of protection are used in the suggested method to protect clients' confidential information. The first layer is to determine whether the website is legal or illegal website .If the site were visited by actual people, they could examine the image captcha to determine whether they were authorized to access it or not. Therefore, no machine client may split the secret word or other sensitive data of the customers using the photo Captcha approach. Additionally, it prevents attacks on the user's account by attackers as a third layer of security. When a client knows a specific client's username, this tactic provides additional protection by preventing unauthorized users from accessing the account. The proposed strategy is additionally valuable to anticipate the assaults of phishing websites on monetary web entrance, keeping money entry, and online shopping advertising.



VI. CONCLUSION

In conclusion, the proposed authentication method using image processing and improved steganography in the banking industry presents an innovative approach to address the challenges of verifying customer identity while enhancing security against potential data breaches. By generating shares that hide the password within an image, the system reduces the risk of storing sensitive information directly in the database.

The key advantages of this approach include:

Improved Security The hidden password within the shares makes it challenging for unauthorized parties to gain access to sensitive information, even if the database is compromised.

Reduced Data Exposure: Storing only shares in the database rather than actual passwords or sensitive data minimizes the exposure of critical information, reducing the potential impact of a breach.

UserFriendly: From the user's perspective, the authentication process can be relatively straightforward, involving the presentation of their share during transactions.

VII. FUTURE WORK

Algorithm refinement : continue research and development to

Improve the image processing and stegnography algorithms used in the system .focus on increasing the complexity of the

hiding process to make it more robust against potential attacks

Performance Optimization: Optimize the decoding process and image reconstruction to minimize latency during transactions, ensuring a seamless and efficient user experience.

User Experience (UX) Study: Conduct thorough UX studies and gather feedback from customers to identify any potential usability issues and improve the overall user experience. User acceptance and ease of use are critical factors in the success of any authentication system.

Resistance to Attacks: Perform extensive security testing, including penetration testing and vulnerability assessments, to identify potential weaknesses and fortify the system against attacks like brute force, collusion attacks, or reverse engineering attempts.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207173 |

Integration with Mobile Apps: Develop mobile applications that allow customers to access their shares conveniently and securely on their smartphones, enabling seamless transactions from any location.

Blockchain Implementation: Investigate the possibility of using blockchain technology to enhance the system's security, transparency, and traceability. Blockchain can provide an immutable record of share transactions, further enhancing the trustworthiness of the authentication process.

Overall, the future work for this project should aim to refine and enhance the proposed authentication method, ensuring it meets the highest standards of security, usability, and regulatory compliance. Continuous research and development, along with proactive testing and collaboration with industry experts, will be instrumental in making this method a reliable and widely adopted solution for secure customer authentication.

REFERENCES

[1] Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; ”Anti-Phishing Tech- nique using Automated Challenge Response Method’”, in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.
[2]”A DNS based Anti-Phishing Approach,” in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Com- munications and Trusted Computing, 2010
[3]T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,. in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41- 43.
[4]Haijun Zhang , Gang Liu, and Tommy W. S. Chow, “Textual and Vi- sual Content-Based Anti-Phishing:A Bayesian Approach,” IEEE Trans. Neural Netw., vol. 22, no. 10, pp. 1532–1546, Oct. 2011.
[5]W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications,. IEEE Transactions, ISCAS-2004, pp. 572- 575.
[6]Monrose, F., Rubin, A. (2001). Use of shared, distributed visual cryptography to support the recall. In Security and Watermarking of Multimedia Contents (Vol. 4314, pp. 248-261).
[7]Naor, M., Shamir, A. (1994). Visual cryptography. In Advances in Cryptology - EUROCRYPT ’94 (pp. 1-12). Springer Berlin Heidelberg.
[8]Kafri, O., Keren, D., Herczeg, Y. (2001). Visual cryptography for general access structures. Computers Security, 20(6), 506-519.
[9]G. R. Blakley, ”Safe guarding cryptographic keys”, in Proceedings of the 1979 AFIPS National Computer Conference, 1979, pp. 313317.
[10]Schoenmakers B., ”A simple publicly verifiable secret sharing scheme and its application to electronic voting,” Advances in Cryptology - CRYPTO’99, Springer Verlag, 1999, pp. 148-164.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details