JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhancing Digital Security: A Dual-Layer Approach with Biometric Authentication and Image-Based Passwords

Jitendra Kumar Katariya[1] , Ankit Kumar[2] , Vinay Kumar[3] , Abdul Rashid[4], Anjali Kumari[5] , Ajay Singh Shekhawat[6]

Scholar[2,3,4,5,6] , Assistant Professor[1]

Department of Computer Science and Application , Vivekananda Global University , Jaipur

Abstract : In today's digital era, organizations rely on online platforms for data management, necessitating stringent user authentication measures. Our proposed solution advocates for a dual-layer security system combining biometric authentication and image-based passwords. Users register using biometric fingerprints, with enhanced security through SHA-512 specifications. This process is followed by dynamic picture selection to create unique validation patterns, proving more effective than existing methods. Additionally, a set of four keys ensures secure data transfer, bolstering overall system security. Rigorous validation of access patterns confirms the system's reliability, positioning it as a trustworthy solution for secure data exchange.

IndexTerms **Digital security, dual-layer approach, biometric authentication, image-based passwords, SHA-512, dynamic validation, secure data transfer.**

I. INTRODUCTION

In today's digital landscape, the escalating frequency and sophistication of cyber threats have emerged as formidable challenges to the security of digital information [1]. Data breaches, identity theft, malware infections, and phishing attacks are just a few examples of the diverse array of threats facing individuals, organizations, and governments worldwide. These threats not only jeopardize the confidentiality, integrity, and availability of digital assets but also undermine trust in digital systems and erode the fabric of society [1]. The increasing reliance on digital technologies across various sectors, including finance, healthcare, and government, further exacerbates these challenges. As technology continues to evolve rapidly, so too do the tactics and capabilities of cyber adversaries, highlighting the urgent need for robust and adaptive security measures [1].

In light of these challenges, the importance of adopting a dual-layer approach to digital security becomes increasingly evident. Traditional security mechanisms, such as password-based authentication, often prove inadequate in the face of sophisticated attacks. A single layer of security is inherently vulnerable to exploitation, as evidenced by the prevalence of password breaches and account compromises [2]. In contrast, a dual-layer approach leverages multiple layers of security to create a more resilient defense against cyber threats. This concept, known as defense in depth, recognizes that no single security measure is foolproof and seeks to mitigate risk through redundancy and diversity. By combining complementary layers of security, such as biometric authentication and image-based passwords, organizations can significantly enhance their ability to detect, prevent, and mitigate cyber attacks [2].

The significance of the dual-layer approach lies in its ability to address the limitations of traditional security measures and provide a more comprehensive and adaptive defense against modern cyber threats [3]. Biometric authentication offers a high level of assurance by verifying an individual's unique physiological or behavioral characteristics, such as fingerprints, iris patterns, or voiceprints. In contrast, image-based passwords leverage visual cues and spatial relationships to create memorable yet secure authentication mechanisms. By integrating these two layers of security, organizations can achieve a balance between usability and security, enabling users to access digital resources conveniently while minimizing the risk of unauthorized access [3].

Against this backdrop, the objectives of this paper are twofold: to propose a novel dual-layer security approach that leverages biometric authentication and image-based passwords, and to evaluate the effectiveness of this approach in enhancing digital security [4]. Through empirical studies or simulations, this research aims to assess the strength, reliability, and usability of the proposed security architecture. Additionally, the paper seeks to provide practical recommendations for implementing and deploying dual-layer security solutions in real-world environments. By addressing these objectives, this research endeavors to contribute to the advancement of cybersecurity practices and support the ongoing efforts to secure digital infrastructure in an increasingly interconnected world [4].

II. Literature Review

Shah Zaman Nizamani, Tariq Jamil Khanzad, Syed Raheel Hassan, Mohd Zalisham Jali [5] The authors discuss the vulnerability of literary passwords in computer systems due to attacks like spyware and dictionary attacks. They propose graphical password schemes as a solution to enhance password security against offline attacks, without requiring users to remember new types of passwords.

Mohammed A. Fadhil Al-Husainy, Diaa Mohammed Uliyan [6] Authentication methods, particularly Personal Identification Numbers (PINs), are susceptible to malicious attacks. The authors introduce a literary password authentication scheme as an alternative to graphical passwords, aiming to provide a more secure login session for users without the need for traditional keyboard inputs.

Desai, Ninaad Suvarna, Dipen Desai, Simranjeet Singh Chawla, Prof. Sowmyashree [7] Literary passwords are widely used for authentication, but they are vulnerable to various attacks. The authors propose two authentication methods based on text and colors for PDAs, generating session passwords resistant to dictionary and brute force attacks.

Sura Jasim Mohammed [8] In the context of increasing data sharing and web transactions, the author proposes an automated password generation method based on initial data input. The generated passwords are non-guessable and suitable for various applications, without burdening users with remembering them.

Anjali Somwanshi, Devika Karmalkar, Sachi Agrawal, Poonam Nanaware, Mrs. Geetanjali Sharma [9] The authors highlight the importance of IT infrastructure security and propose a system to address specific attacks like keystroke logging and shoulder surfing, thus enhancing login security mechanisms.

M I Awang, M A Mohamed, R Mohamed, An Ahmad, N A Rawi [10] The authors address the vulnerability of literary passwords to attacks like shoulder surfing. They propose a pattern-based password authentication system, where users select and enter passwords based on predefined patterns during login, improving security against such attacks.

B. S. A. Kumar, A. S. L. C. S. Kumari [11] The authors discuss issues in spatial database keyword retrieval and propose a new algorithm to address these problems, extending nearest keyword search to handle inter-object distance and keyword rating for better object evaluation.

Z. Bao, J. Lu, T. W. Ling, B. Chen [12] Inspired by successful keyword search techniques on the web, the authors propose a framework for keyword search on XML. They introduce specific guidelines and novel ranking methods for search engines to improve search result relevance and effectiveness.

III. Research Methodolgy

The research methodology proposed in the provided algorithm outlines the steps and procedures for user authentication and secure data transmission in a computer system. It encompasses several key components, including new user registration, existing user login, key formation for data sending, and data receiving by the recipient.

1. **New Users Registration:** This phase involves registering new users into the system. It begins with collecting user information such as name and email ID. The user's biometric fingerprint is then selected and processed using the SHA-512 algorithm to generate a unique hash code. The user selects images for authentication and segments of those images. Finally, a pattern is generated based on the selected images and segments, and the user's details are stored in the database.

2. **Existing Users Login:** In this phase, existing users authenticate themselves to access the system. Similar to the registration process, the user's biometric fingerprint is processed using the SHA-512 algorithm to generate a hash code. The user selects images for authentication and segments of those images. A pattern is generated based on the selected images and segments, and the system validates the user's details against the database to grant access.

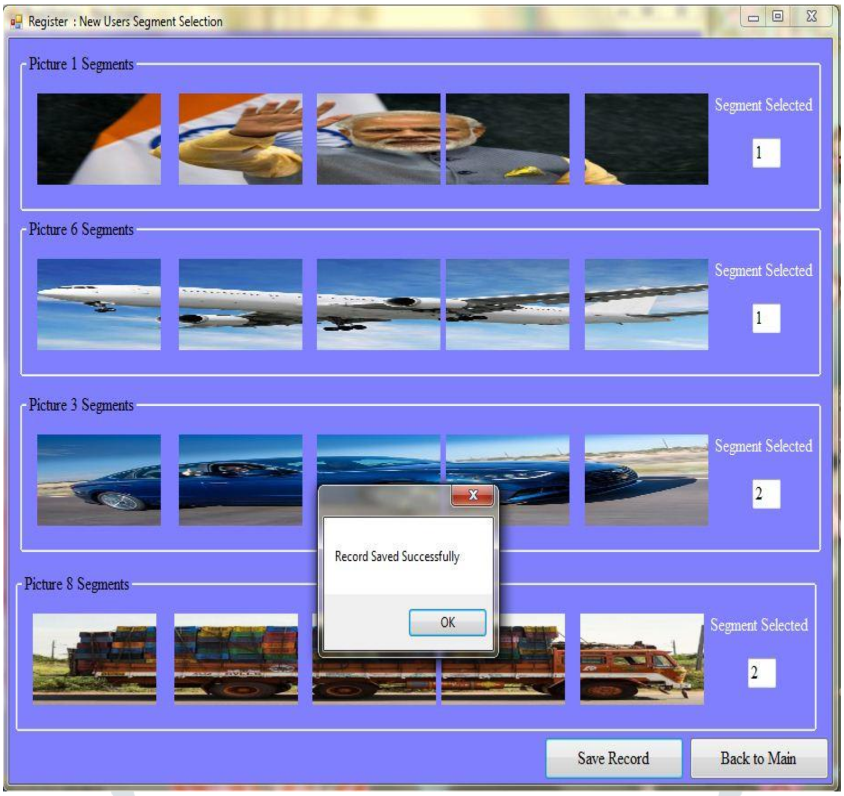
3. **Keys Formation for Data Sending:** This phase focuses on generating keys for secure data transmission between users. The sender selects the recipient from a list of existing users and chooses images for picture-based keys. Private keys are generated using random numbers, and a combination key is created using SHA-512 extracts of both users' biometric data. The sender enters the message to be sent, and the details are saved in the database, including a unique message sequence number.

4. **Receiving Data from Sender:** In this phase, the recipient retrieves the data sent by the sender. The recipient enters the message sequence number and selects images for picture-based keys. Private keys and the combination key are inputted, and the system validates the details against the database. If validated, the message is fetched from the database.

Overall, this methodology employs a multi-layered approach combining biometric authentication, image-based passwords, and cryptographic keys to ensure secure user authentication and data transmission in the system.

.

IV. Simulations and Result Analysis



Picture 1 Segments — Segment Selected: 1

Picture 6 Segments — Segment Selected: 1

Picture 3 Segments — Segment Selected: 2

Picture 8 Segments — Segment Selected: 2

Record Saved Successfully

Fig 4.1 Implementation

In our approach we have take two main keys , one is the combination key which is formed by the SHA extract of the finger print and second is the pattern form on the basis of the graphical picture selection and the segments selection.

For example we have take ,

Combination Key : beccd58d34_88a1d01e1e

Graphical Based Pattern :

Picture1_Partition1_Picture6_Partition1_Picture3_Partition2_Picture8_Partition2_1122

Tool 1 "How Secure Is My Password?"

Tool 2 "Take the Password Test"

Table 4.1 Text Password Comparison Tool 1

Base Result	Proposed Result
109 years	5 hundred quadrillion years

Table 4.2 Graphical Password Comparison Tool 2

Base Result	Proposed Result
339years	2 hundred quadrillion quadragintillion years

V. Conclusion

In today's digitally-driven world, where organizations rely heavily on online data and communication systems, user validation is crucial to ensure the security of sensitive information. The proposed approach in this work aims to provide a robust method for user validation and secure information sharing. By registering users using biometric fingerprints and utilizing the SHA-512 algorithm for fingerprint specification, a dynamic extract of the SHA hash is incorporated into the validation process, enhancing security.

Furthermore, the validation process involves selecting dynamic pictures and segments, resulting in the formation of a unique pattern for each user. Comparative analysis with existing methods demonstrates the effectiveness of the proposed approach. Additionally, the use of four keys, including message sequence number, random number-based private keys, picture selection-based keys, and combination keys based on SHA fingerprint hash, further enhances the security of the data transfer process.

Future Work:

In future endeavors, there are several avenues for further exploration and enhancement of the proposed approach. Firstly, the implementation of the proposed approach in various security models will be pursued to assess its adaptability and effectiveness across different contexts. Additionally, research will be conducted into emerging segments of cryptography and password authentication, such as Quantum cryptography and Retina-Based Passwords, to stay at the forefront of technological advancements and continually improve security measures. These future endeavors aim to further strengthen the security of user validation and data transmission in digital systems..