IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PICTOGRAM AUTHENTICATION

Revolutionizing Security: Pictogram Authentication Unleashes the Power of Visual Recognition

[1]K. Yashodha Pavani, [2]A. Bharath Varma, [3]P. Gowtham,[4] Ramalinga Swamy M V S, [5]P.V.S. Manisha,

[1-4] B.Tech Student, [5]Assistant Professor

[1,2,3,4,5]Computer Science And Information Technology,

[1,2,3,4,5]Lendi Institute of Engineering and Technology, Vizianagaram, India.

Abstract: The Pictogram authentication system represents an avant-garde paradigm in user verification, harnessing the cognitive strength of visual symbols. This project proposes a cutting-edge authentication system, accentuating visual password creation, pattern recognition, and fortified security protocols. Key components encompass user-friendly interactions, multimodal integration, scalability, and rigorous usability testing. Developed with Java, Python, HTML, CSS, and JavaScript for web-based interfaces, the project employs analytical tools like R, Matplotlib, and Seaborn for robust performance evaluation. The system not only prioritizes security enhancement but also addresses user education, ensuring a seamless blend of accessibility and human-centric design. In summary, this project pioneers a secure, visually-driven authentication solution, harnessing innate human visual recognition capabilities for a resilient and inclusive digital future.

***Index Terms*-Visual Password, Security Enhancement, Digital Authentication**

I. INTRODUCTION

In the rapidly evolving landscape of user authentication, the Pictogram authentication system emerges as a groundbreaking paradigm, tapping into the cognitive prowess of visual symbols and icons. This project endeavors to revolutionize authentication methodologies by introducing an innovative system, placing a premium on visual password creation, pattern recognition, and fortified security measures. The initiative encompasses critical facets such as user-friendly interactions, multimodal integration, scalability, and meticulous usability testing. Developed through a tech stack encompassing Java, Python, HTML, CSS, and JavaScript for web-based interfaces, augmented by analytical tools like R, Matplotlib, and Seaborn, the project not only prioritizes security enhancement but also underscores the significance of user education. In pursuit of a harmonious blend of accessibility and human-centric design, the system pioneers a secure, visually-driven authentication solution, poised to shape a resilient and inclusive digital future..

II. LITERATURE SURVEY:

The literature survey delves into advanced password authentication methods. Zheng and Jia introduce CombinedPWD, utilizing separators to bolster security [1]. Yusuf presents a dynamic password authentication scheme with user-defined time-based changes [2]. Yang proposes a secure strong password authentication protocol, distinguishing between weak and strong authentication schemes [3]. Wang and Guo offer DPAC, a framework improving password security through countermeasures [4]. Refish introduces PAC-RMPN, facilitating authentication between users through password propagation [5]. Zaki and Husain contribute a secure pattern-key-based password authentication scheme [6]. Pagar and Pise focus on fortifying password security using honeyword and honey encryption techniques [7]. Gurav et al. address graphical password authentication with a cloud-securing scheme [9]. Bianchi et al. propose a secure haptic keypad, a tactile password system [10]. von Zezschwitz et al. explore the impact of mobile devices on password composition

and authentication performance. Sood et al. analyze the cryptanalysis of password authentication schemes, highlighting current status and key issues [8]. Additionally, several references provide comprehensive insights into evolving trends in password authentication [10].

Challenges:

Present password authentication systems encounter numerous challenges. Users often create weak passwords, making them susceptible to brute-force attacks. The widespread practice of password reuse amplifies risks, as compromised credentials can be exploited across multiple accounts. Cyber threats, such as credential stuffing and phishing attacks, continue to exploit human vulnerabilities. Biometric authentication, while convenient, is not foolproof and can be compromised. Forgotten passwords contribute to frequent resets, potentially exposing security vulnerabilities. Resistance to overly complex security measures and the lack of widespread adoption of two-factor authentication further exacerbate these challenges. Addressing these issues necessitates a comprehensive approach that combines technological enhancements, user education, and improved authentication practices.

III. EXISTING SYSTEM

Existing systems for alpha-numeric passwords encompass traditional methods, passphrases, and randomly generated combinations to enhance security. Password policies enforced by organizations often mandate the inclusion of alphanumeric characters. Multi-word passcodes and biometric enhancements provide alternatives for stronger yet memorable authentication. Two-factor authentication systems combine alphanumeric passwords with secondary methods for added security. Smart cards, tokens, and adaptive authentication systems contribute further layers of protection. Integrating behavioral analysis and adaptive security measures, these systems aim to strike a balance between robust security protocols and user-friendly experiences.

Challenges with alpha-numeric passwords include users struggling with memorability and resistance to complexity, leading to security risks. Common pitfalls involve password reuse, predictability, and susceptibility to brute-force attacks, emphasizing the need for user education and a balance between security and usability. Additionally, social engineering and biometric vulnerabilities underscore the multifaceted nature of challenges in maintaining robust alpha-numeric password systems.

IV. PROPOSED SYSTEM

The proposed system for Pictogram Authentication is a pioneering approach that leverages visual symbols and icons for user verification, enhancing security and user-friendly interactions. The key components of the system include visual password creation, pattern recognition, enhanced security measures, user-friendly experiences, accessibility, and multimodal integration. Usability testing ensures an intuitive and effective authentication process, considering user behaviors. Developed using Java, Python, HTML, CSS, and JavaScript, with additional tools like R and Python libraries for behavior analysis, the system incorporates a novel time-based unique password to avoid third-party dependencies. The authentication process involves users embedding separators (e.g., spaces) into passwords during registration, enhancing security. The proposed system not only focuses on security enhancement but also prioritizes accessibility, ease of use, and adaptability to evolving security needs for a more secure and accessible digital future.

V. TECHNOLOGIES

The development of a Pictogram Authentication system involves a combination of technologies to create a secure and user-friendly authentication solution. Here are the key technologies that may be involved in implementing Pictogram Authentication:

5.1. Programming Languages:

- Java: Used for server-side development, backend logic, and business logic.
- Python: Employed for various purposes, including backend development, data analysis, and machine learning.

5.2. Web Technologies:

- HTML (Hyper Text Markup Language): Used for creating the structure of web pages.
- CSS (Cascading Style Sheets): Employed for styling and layout of web pages.
- JavaScript: Enables dynamic and interactive features on the client side.

5.3. Database Management:

- Database (e.g., MySQL, PostgreSQL): Stores user credentials, visual passwords, and other relevant data securely.

5.4. User Interface (UI) Frameworks:

- Frontend Frameworks (e.g., React, Angular, Vue.js): Aid in building dynamic and responsive user interfaces.

5.5. Security Protocols:

- Encryption Algorithms (e.g., AES, RSA): Used to encrypt and secure user credentials during storage and transmission.
- Hashing Algorithms (e.g., SHA-256): Applied for secure one-way hashing of passwords.

5.6. Pattern Recognition:

- Computer Vision Libraries: May be employed for image processing tasks.

These technologies collectively contribute to the development, security, usability, and scalability of the Pictogram Authentication system. The specific tools and frameworks may vary based on the project requirements and development preferences.

V. ARCHITECTURE DIAGRAM AND FLOW CHART

LSTM (Long Short-Term Memory) is a recurrent neural network specialized for sequential data, excelling in tasks like time series prediction and natural language processing. CNN (Convolutional Neural Network) is a feedforward network designed for grid-like data, particularly effective in image-related tasks. Combining LSTM and CNN in hybrid architectures is common for tackling complex problems involving both sequential and spatial data.

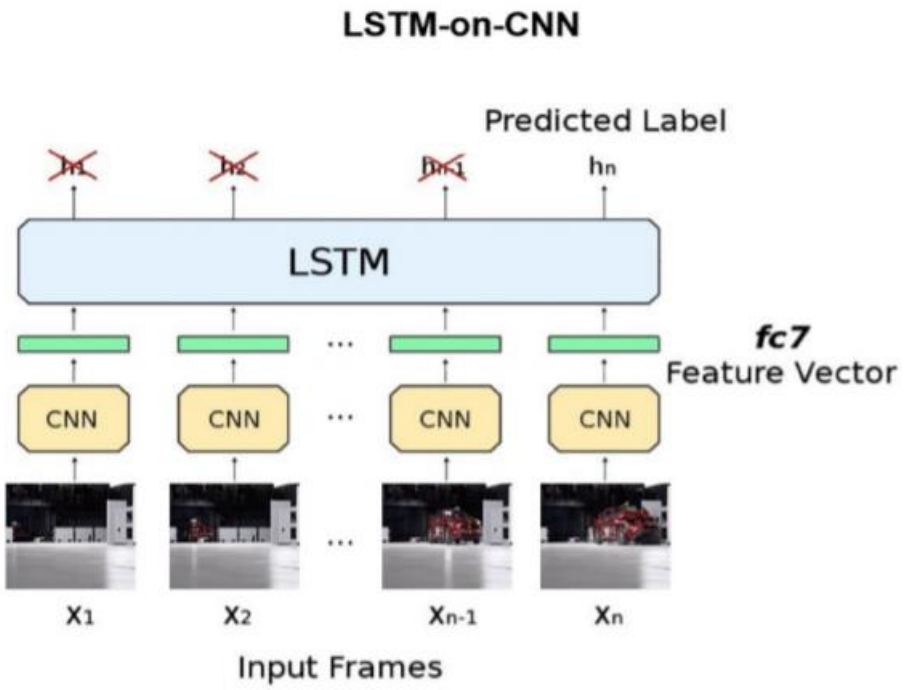

Fig 1: Architecture Diagram

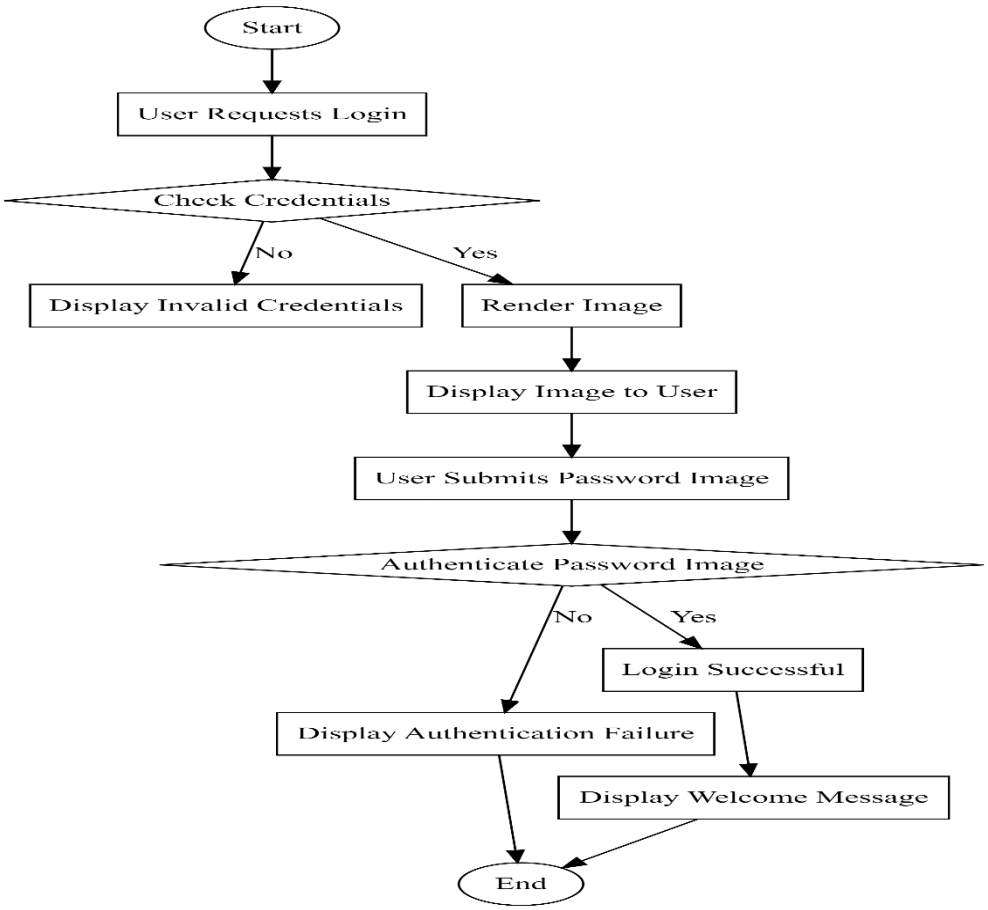

Fig 2: Flow Chart

VII. CONCLUSION

Pictogram Authentication project highlights the development of a novel authentication system based on pictograms, aiming to enhance security while maintaining user-friendly interactions. The project successfully addresses the weaknesses associated with traditional password-based authentication, providing a more secure alternative. By leveraging visual symbols and icons, the system capitalizes on human visual recognition capabilities. The use of technologies such as Java, Python, HTML, CSS, and JavaScript for web-based interfaces, along with tools like R or Python libraries for analysis, contributes to the project's robustness. Overall, the Pictogram Authentication project offers a promising solution for secure and accessible user authentication in the digital landscape.

ACKNOWLEDGEMENT

We would like to thank the Department of Computer Science and Information Technology, Lendi Institute of Engineering and Technology, Vizianagaram for helping us to carry out the work and supporting us all the time.

REFERCENCES

1. Wantong zheng, Chunfu Jia, Combined PWD: A New Password Authentication Mechanism Using Separators Between Keystrokes: 2017 13th International Conference on Computational Intelligence and Security (CIS)
2. Salisu Ibrahim Yusuf, Moussa Mahamat Boukar, User Define Time Based Change Pattern Dynamic Password Authentication Scheme, 2018 14th International Conference on Electronics Computer
3. Yang Jingbo, Shen Pingping, A secure strong password authentication protocol, 2010 2nd International Conference on Software Technology and Engineering

4. Hua Wang, Yao Guo, Xiangqun Chen, DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security, 2008 11th IEEE High Assurance Systems Engineering Symposium
5. Salah Refish, PAC-RMPN: Password Authentication Code Based RMPN, 2018 International Conference on Advanced Science and Engineering
6. M Hamza Zaki, Adil Husain, M Sarosh Secure pattern-key based password authentication scheme2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)
7. Vasundhara R Pagar, Rohini G Pise, Strengthening password security through honeyword and Honey encryption technique, 2017 International Conference on Trends in Electronics and Informatics (ICEI)
8. 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.
9. S. Gurav, L. Gawade, P. Rane, and N. Khochare, Graphical password authentication: Cloud securing scheme, in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479483
10. A. Bianchi, I. Oakley, and D.S. Kwon, The secure haptic keypad: A tactile password system, in Proceedings of the SIGCHI Conference on Human Factors in Computing System. CHI 10. New York, NY, USA: ACM, 2010, 10891092.E. von Zezschwitz, A. De Luca, and H. Hussmann, Honey, shrunk the keys: Influences of mobile devices on password composition and authentication performance.