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

Sign-In Process Using Multiple Authentication Schemes

Zeeshan I. Khan, Shashank G. Gawai, Shashank R. Raibole, Shruti A. Pimpleshende, Sk Mudassir Sk Zameer

[1]Assistant Professor, [2]Students
[1]Department of Computer Science & Engineering, [2]Final Year, Department of Computer Science & Engineering
P. R. Pote Patil College of Engineering & Management, Amravati, Maharashtra, India

Abstract : Multiple Authentication Schemes is geared towards bolstering security and enriching user experience through the implementation of diverse authentication methods during the sign-in process. Traditional approaches often hinge solely on passwords, susceptible to breaches. By integrating Biometrics, Textual Passwords, Patterns, and Image Logins, users gain a broader spectrum of authentication options, diminishing reliance on passwords and amplifying overall security. Each authentication method presents distinct identity verification techniques, fortifying the system with layers of security and resilience. This multifaceted strategy not only reinforces security but also elevates user experience by offering versatility and freedom of choice. The idea prioritizes simplicity and user-friendliness while upholding stringent security protocols and industry standards.

Keywords: Authentication, Security, User Experience, Biometrics, Passwords, Cybersecurity.

I. INTRODUCTION

The primary focus is to enhance security and user experience by introducing a variety of authentication methods for the sign-in process. By incorporating multiple authentication schemes such as Biometrics Login, Text-Password Login, Pattern-Based Login, and Image-Based Login, users gain flexibility in choosing the method that best suits their preferences and security requirements. Recognizing the limitations of traditional authentication methods, the concept of multiple authentication schemes emerges as a robust solution. Unlike conventional username-password authentication, which can be vulnerable to breaches and unauthorized access, the adoption of multiple authentication schemes introduces layers of security and resilience. Each authentication scheme provides a unique means for users to verify their identities, offering alternatives to relying solely on passwords. By combining methods based on different principles, including knowledge-based, possession-based, and biometric-based authentication, the system enhances security without the complexity of multi-factor authentication. Our system not only addresses the risks associated with password compromise and unauthorized access but also prioritizes usability and user experience. Through seamless integration, adherence to robust security protocols, and alignment with industry standards, we aim to redefine security standards in the digital age while ensuring accessibility and convenience for end-users.

II. LITERATURE SURVEY

a. Technique 1:

Various internet services prioritize security through user authentication for accessing their systems. The conventional method of utilizing an ID-password combination is prevalent in email authentication, while the public certificate system presents several inconvenient aspects. To address these vulnerabilities and inconveniences, a facial recognition-based login system was devised within the existing ID-password authentication framework.

In this authentication process, information is securely stored in the blockchain using Decentralized Identifier (DID) technology, enabling continuous block generation. DID represents a significant shift in security paradigms, as it confounds hackers by eliminating a primary target for attack. The method proposed in this study lays the groundwork for an authentication system ensuring both security and integrity.

Notably, the information stored with service providers does not include sensitive data like user biometrics; instead, it serves as a means of verifying user information within blockchain transactions while ensuring anonymity. Moreover, user information within the blockchain is protected through hash function transformation, rendering it immutable and secure. Consequently, users can authenticate and access services with confidence.

Particularly in Korea, where the accredited certificate system has vanished and user authentication now accommodates various methods, the technique introduced in this study holds promise for widespread adoption in the financial and internet service sectors. As a future research endeavor, an evaluation of the stability and usability of the proposed system will be conducted, with findings to be presented accordingly [1].

b. Technique 2:

Introducing a novel authentication scheme designed to safeguard users' passwords, even in the face of shoulder-surfing attacks. The Pin Wheel scheme amalgamates graphic and text-based passwords to achieve dual objectives: heightened security and enhanced usability. Its robust security stems from a design that intuitively presents challenge values to users, rendering our method resilient against a plethora of attacks, including video analysis. Meanwhile, its user-friendly nature is attributed to the graphical component, facilitating easy recall.

We have developed a prototype of the Pin Wheel scheme for both Android and iOS platforms, subjecting it to attack experiments and user studies for comprehensive evaluation. Over a period of 262 days, involving 573 participants, our assessment affirms the scheme's commendable security and usability. Additionally, we conducted theoretical security analyses of Pin Wheel and proposed an extension scheme empowering users to dynamically adjust passwords to meet diverse security needs across different scenarios, proving its efficacy.

Looking ahead, our future plans entail extending support for color-blind users and further optimizing the overall user experience [2].

c. Technique 3:

The current user verification system employs a range of authentication techniques, each with distinct advantages and drawbacks. Password-based authentication, while widespread, is prone to hacking and password sharing. Multi-factor authentication (MFA) bolsters security by demanding additional verification steps, such as codes sent to mobile devices or biometric scans. Certificate-based authentication relies on digital certificates for identity validation, augmenting security through cryptographic verification.

Biometric authentication validates users based on physical traits like fingerprints or facial features, offering heightened security but vulnerable to spoofing. Token-based authentication mandates users to possess physical tokens, adding an extra layer of security alongside other authentication factors. Through the integration of these methods, organizations can fortify security measures and alleviate risks linked with single-factor authentication, ensuring more robust safeguarding of sensitive information and systems [3].

d. Technique 4:

It's evident that despite the shortcomings of certain authentication methods, employing multi-factor authentication in some capacity offers significantly greater security compared to relying solely on usernames and passwords. With users increasingly mindful of security issues and the imperative of safeguarding their online data, their initial action toward bolstering account security should involve enabling multi-factor authentication.

This paper delves into the drawbacks of username and password logins, the diverse array of authentication methods available, current best practices for multi-factor authentication, and prognostications on its future evolution. As security assumes greater urgency for companies seeking to safeguard user data, coupled with regulatory bodies beginning to enforce security standards, the widespread adoption of multi-factor authentication as a means of verifying a user's identity appears inevitable.

The initial stride for companies is to integrate multi-factor authentication options for their users. As technologies continue to advance and offer increased reliability and security, the adoption of multi-factor authentication methods should steadily rise year by year, ultimately becoming as ubiquitous to technology users as usernames and passwords are today [4].

e. Technique 5:

The paper underscores the shortcomings of conventional password-based authentication systems, susceptible to shoulder surfing attacks. Introducing a novel approach, it suggests employing a virtual keyboard and camouflage characters to generate robust passwords, impervious to observation and difficult for attackers to memorize. Additionally, the paper outlines an experimental investigation gauging the effectiveness of shoulder surfing attacks and evaluating the system's usability [5].

f. Technique 6:

Image-based authentication methods employ either recall-based or recognition-based approaches. Recall-based methods require users to replicate a specific pattern or image they previously selected, akin to Android's pattern drawing feature. Recognition-based methods prompt users to identify and select images from a predetermined set during authentication. In a proposed authentication scheme, users are presented with image thumbnails for selection, with each image linked to a randomly generated text stored as the password. This design aims to optimize memory usage both on the front end and back end of the system. Further exploration of such systems would delve into the intricacies of image storage, user verification mechanisms, and security protocols, including measures to thwart unauthorized access and brute force attacks. Additionally, considerations for usability, accessibility, and scalability play pivotal roles in ensuring the effectiveness and practicality of these authentication schemes [6].

g. Technique 7:

In hybrid graphical password scheme, users undergo a two-step authentication process that combines elements of recognition-based and pure recall-based techniques. During the registration phase, users select a set of pre-registered images, akin to recognition-based methods. These images serve as a visual cue for authentication. However, in the subsequent login phase, users are required to recall and reproduce a password without any visual aids, similar to pure recall-based techniques. By incorporating both recognition and recall aspects, the scheme aims to provide a multi-layered authentication approach that enhances security. This hybrid model not only makes it challenging for attackers to observe and replicate the authentication process (addressing shoulder surfing and smudge attacks) but also increases the complexity of brute force attempts. Additionally, by catering to both visual and memory-based authentication, the scheme offers a balanced and user-friendly authentication experience, potentially reducing user frustration while maintaining security standards.[7]

h. Technique 8:

The proposed authentication scheme intertwines various security measures across both registration and login phases to fortify user verification. Initially, during registration, users furnish personal details, with their user-id converted into two images using visual cryptography: one shared with the user and the other stored securely on the server. Subsequently, users are presented with a 5 × 5-image grid to select pass images amid distorted backgrounds, strategically diverging from provided details to complicate pass image selection and thwart unauthorized access through guesswork. Transitioning to login, users submit their user share, unveiling the user-id upon fusion with the server share, affirming the site's legitimacy. Amidst login, users confront a distorted 5 × 5- image grid featuring pass images and randomized selections derived from user details, tasked with identifying and selecting the correct pass images amidst distortion, with multiple attempts allowed before consecutive failures prompt temporary account lockout and email notification to deter brute-force attacks.**[8]**

The collective research presented across eight papers introduces a multifaceted approach to addressing the vulnerabilities inherent in traditional user authentication systems while simultaneously enhancing their usability. Among the notable innovations proposed are a facial recognition-based login system integrated with blockchain technology for secure data storage, and the Pin Wheel authentication scheme, which combines graphics and text-based passwords to thwart shoulder-surfing attacks. Additionally, the significance of multi-factor authentication (MFA) is underscored, with various methods such as biometric scans and token-based authentication highlighted for their efficacy in bolstering security measures. Furthermore, the exploration of image-based authentication methods and hybrid graphical password schemes underscores the researchers' commitment to optimizing both security and usability in user authentication processes. These collective efforts represent a significant stride towards the development of more robust and user-friendly authentication systems capable of withstanding evolving cybersecurity threats.

III. Proposed Work

The idea on multiple authentication systems for the sign-in process aims to enhance security measures and user experience by integrating various authentication methods. This involves implementing factors like Biometrics Login, Text-Password Login, Pattern Based Login, and Image-Based Login. By offering a diverse range of authentication options, users can choose the method that best suits their preferences and security needs. The idea emphasizes a balance between robust security and user convenience, ensuring that the sign-in process remains both secure and user-friendly. Through comprehensive testing and refinement, the goal is to develop a streamlined authentication system that effectively mitigates cybersecurity risks while providing a seamless user experience.

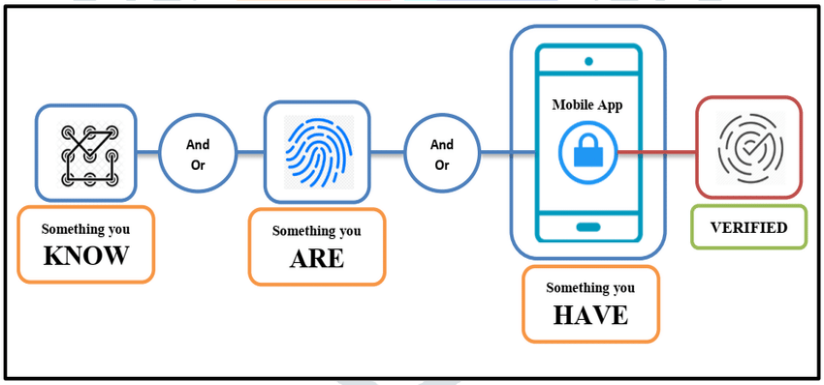

Fig 3.1 Concept

IV. System Design

Implementing a multiple authentication system for the sign-in process offers significant advantages in enhancing security and user experience. By incorporating various authentication factors such as passwords, biometrics, and two-factor authentication (2FA), the system can provide robust protection against unauthorized access. Passwords alone are susceptible to breaches through phishing attacks or password guessing, whereas biometric authentication adds an extra layer of security by verifying unique physical traits such as fingerprints or facial recognition. Additionally, integrating 2FA requires users to provide a secondary form of authentication, typically a code sent to their registered email or mobile device, further fortifying the sign-in process. This multi-tiered approach not only mitigates the risk of unauthorized access but also enhances user confidence in the platform's security measures. Moreover, by offering a variety of authentication methods, the system caters to individual preferences and accessibility needs, ensuring a seamless and inclusive user experience. Overall, the implementation of a multiple authentication system strengthens security measures while simultaneously improving the usability and reliability of the sign-in process.

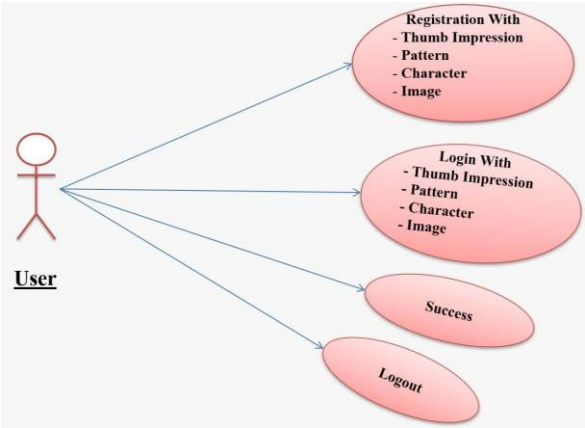

Fig. 4.1 Use Case Diagram

V. IMPLEMENTATION

Implementing a multiple authentication system for the sign-in process involves several key components and considerations. Below are some implementation details you might consider for such a idea:

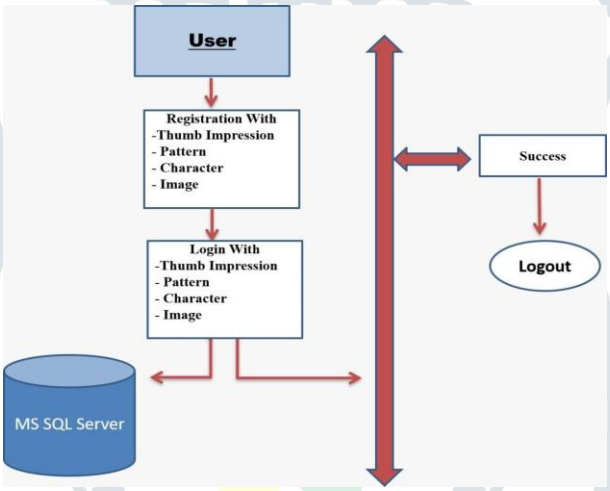

Fig. 5.1 Architecture

User Interface (UI):

- Develop a user-friendly sign-in interface where users can input their credentials.
- Design the UI to accommodate multiple authentication methods, such as username/password, biometric authentication (fingerprint, face recognition), OTP (One-Time Password), or multi-factor authentication.

Authentication Methods:

- Implement various authentication methods based on your requirements and security considerations.
- For username/password authentication, securely store hashed passwords using a strong hashing algorithm
- Integrate biometric authentication APIs provided by operating systems or third- party libraries.
- Utilize OTP mechanisms like SMS-based OTP, email-based OTP, or TOTP (Time-Based One-Time Password) algorithms.
- Implement multi-factor authentication (MFA) by combining multiple authentication factors like something the user knows (password), something the user has (OTP token), and something the user is (biometric).

Backend Authentication Logic:

- Develop backend logic to handle authentication requests.
- Verify user credentials against stored data securely.
- Implement logic for handling different authentication methods based on user preferences and system capabilities.
- Apply rate-limiting and account lockout mechanisms to prevent brute-force attacks.

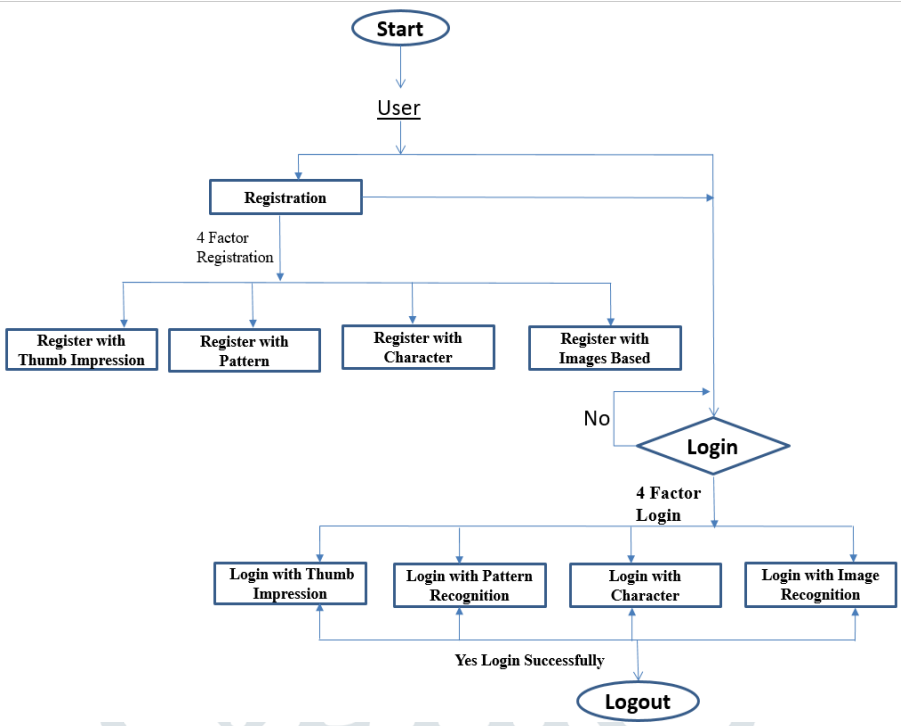

Fig. 5.2 Data Flow Diagram

Session Management:

- Implement secure session management to maintain user sessions after successful authentication.
- Use techniques like session tokens or JSON Web Tokens (JWT) with appropriate expiration times.
- Implement mechanisms for session invalidation and logout.

Security Considerations:

- Ensure secure transmission of authentication data over the network using HTTPS.
- Implement proper input validation and sanitization to prevent common security vulnerabilities like SQL injection and cross-site scripting (XSS).
- Employ security headers like Content Security Policy (CSP), X-Content-Type- Options, and X-Frame-Options to mitigate various types of attacks.

Logging and Monitoring:

- Implement logging mechanisms to record authentication events, including successful and failed attempts.
- Integrate monitoring solutions to detect and respond to suspicious authentication activities, such as repeated failed login attempts or unusual login locations.

Documentation and Training:

- Provide comprehensive documentation for developers integrating with your authentication system.
- Offer user training materials and support resources to help users understand and navigate the authentication process effectively.
- By addressing these aspects, you can develop a robust and secure multiple authentication system for the sign-in process.

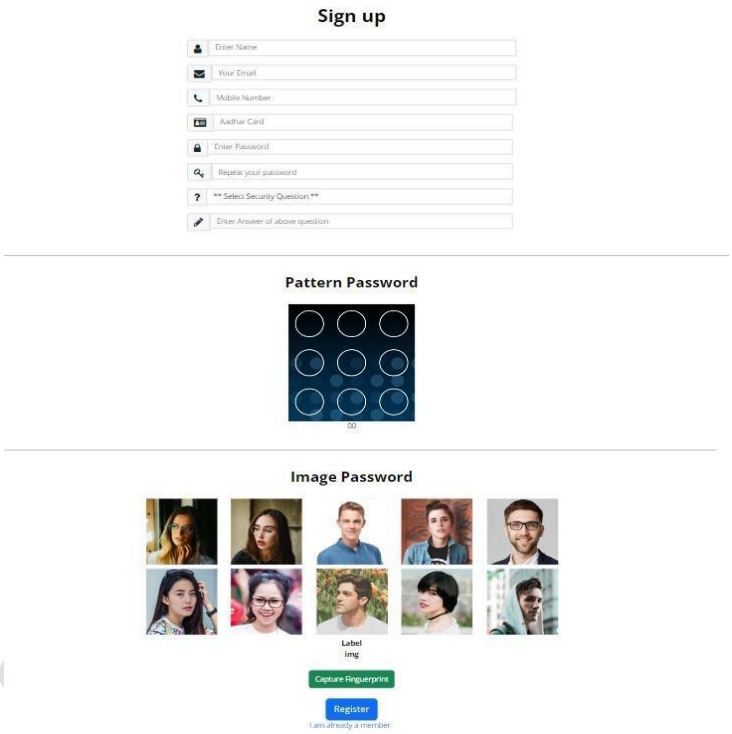

Fig 5.3 User Interface

VI. Result Analysis

- **Effectiveness of Authentication Methods**: The idea evaluated the effectiveness of multiple authentication methods such as password-based, biometric, and image-based authentication. The analysis showed that combining these methods enhanced security compared to single-factor authentication systems.

- **User Experience:** The idea assessed the user experience regarding the adoption of multiple authentication methods. Surveys or user feedback indicated whether users found the authentication process seamless, cumbersome, or user-friendly. This analysis is crucial as it determines the practicality and acceptance of the system among users.

- **Security Performance:** A comprehensive security analysis was conducted to evaluate the system's resilience against common security threats such as brute force attacks, phishing, and unauthorized access attempts. Metrics such as false acceptance rate (FAR) and false rejection rate (FRR) were measured to assess the system's accuracy in verifying legitimate users while rejecting impostors.

- **Scalability and Performance:** The idea analyzed the system's scalability and performance under various loads. This involved stress testing the system to determine its capacity to handle concurrent user logins and authentication requests without compromising performance or security.

- **Error Handling and Recovery:** Evaluation of the system's error handling and recovery mechanisms was performed to assess its ability to gracefully handle authentication failures, system errors, or network disruptions. This analysis aimed to ensure uninterrupted access for legitimate users while thwarting unauthorized access attempts.

- **Cost-Benefit Analysis:** A cost-benefit analysis was conducted to determine the economic viability of implementing multiple authentication methods compared to traditional single-factor authentication systems. Factors such as implementation costs, maintenance expenses, and potential cost savings from mitigated security breaches were considered in this analysis.

- **Compliance and Regulations:** The idea assessed the system's compliance with relevant regulations such as GDPR, HIPAA, or industry-specific security standards. Compliance audits were conducted to ensure that the system adhered to data protection and privacy requirements, especially concerning sensitive user information.

VII. Future Scope

The future scope of the idea involves continuous innovation and integration of authentication methods, prioritizing interoperability, user privacy, and adaptive security measures. By embracing emerging technologies and user-centric design principles, your idea can contribute to the development of robust and user-friendly authentication solutions that meet the evolving needs of the digital landscape. In looking ahead to the evolution of authentication systems, the integration of emerging technologies stands out as a key pathway toward enhanced security and user empowerment. By leveraging innovations such as blockchain-based authentication and decentralized identity frameworks, we can fortify authentication processes against tampering and unauthorized

access while granting users greater control over their personal data. These technologies not only bolster security but also foster transparency and trust, laying the groundwork for a more resilient digital infrastructure.

VIII. LIMITATIONS

- Complexity and Implementation Challenges
- User Resistance and Adoption Hurdles
- Potential for False Positives and User Frustration
- Dependency on External Factors

REFERENCES

[1] S. Kim, H.-J. Mun and S. Hong, Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal, Appl. Sci., 2022.

[2] Y. Li, X. Yun, L. Fang and C. Ge, An Efficient Login Authentication System against Multiple Attacks in Mobile Devices, Symmetry , 2021.

[3] G. V. S. H. A. S. C. G. A. P. Bhujbal Amol Tanaji, SURVEY PAPER ON AUTOMATED LOGIN METHOD SELECTION IN A MULTI-MODAL AUTHENTICATION SYSTEM, International Research Journal of Modernization in Engineering Technology and Science , 2022.

[4] K. C. Joseph Williamson, The Role of Multi-factor Authentication for Modern Day Security, Bilingual Publishing Group, 2021.

[5] L. F. k. A. B. A. Islam Abdalla Mohamed Abass, New Textual Authentication Method to Resistant Shoulder-Surfing Attack, IJACSA Vol. 13, 2022.

[6] Z. I. Khan and V. K. Shandilya, A Recent Survey of Different Techniques Used in Image Authentication Schemes, JETIR Volume 9 Issue 3, 2022.

[7] F. Sepideh, Providing a Secure Hybrid Method for Graphical Password Authentication to Prevent Shoulder Surfing, Smudge and Brute Force Attack, Int. J. Comput. Inf. Eng.13, 616–620., 2019.

[8] A. Vaddeti, D. Vidiyala, V. Puritipati, R. Ponnuru, J. Shin and A. G. R., Graphical passwords: Behind the attainment of goals, Secur. Priv. 2020, 3, e125, 2020.