International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Survey on Graphical Password Strategy Authentication

Shruti Taware[1], Pratik Deshpande[1], Tanaya Deshmukh[1], Anshu Thakur[1], Yogita Pore[2]

[1]Final Year Student, Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India
[2]Assistant Professor, Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT

In an ever-evolving digital realm, ensuring the security and reliability of software applications has become increasingly crucial. The continuous advancement of technology also brings about more complex cyber threats, emphasizing the urgent need to identify and address vulnerabilities. In response to this growing imperative, we introduce "Graphical Password Authenticator: A Novel Approach to Secure User Authentication." The Graphical Password Authenticator reimagines the conventional user authentication process by utilizing graphical elements and innovative techniques. It provides a secure and user-friendly alternative to traditional text-based passwords, offering enhanced protection against unauthorized access. By incorporating graphical images, patterns, or other visual cues, users can create unique and memorable authentication credentials that are difficult for malicious actors to compromise. This approach offers a more intuitive and engaging way for users to access their accounts while significantly reducing the risk of password-related security breaches. The Graphical Password Authenticator system ensures robust security through a combination of graphical recognition and encryption technologies. It is designed to be resistant to common attack methods such as brute force and keyloggers, providing a higher level of protection for user accounts and sensitive information. This novel approach to user authentication fosters a secure and user-centric environment, making it a promising solution for the ever-evolving digital landscape. The Graphical Password Authenticator is a groundbreaking step at the intersection of user authentication and innovation. By redefining the way users prove their identity through memorable graphical elements, this approach empowers users with a more secure and intuitive means of accessing their digital resources. This paradigm shift in authentication methods showcases the potential of technology to enhance user security and create a safer digital future, ultimately bridging the gap between user convenience and robust cybersecurity.

Keywords: Graphical Password Authenticator, User Authentication, Cybersecurity, Digital Security, Encryption Technologies, User-Centric Approach, Brute Force Resistance, Keyloggers Protection.

I. INTRODUCTION

In an age characterized by rapid technological advancement and increasing reliance on digital systems, the importance of robust and user-friendly authentication methods cannot be overstated. The need for secure and intuitive access to digital resources has prompted continuous innovation in the field of authentication, and one such innovation is "Graphical Authentication."

Graphical authentication stands as an innovative approach to user identity verification, departing from traditional alphanumeric passwords and PINs. Instead, it leverages graphical elements, visual cues, or images to provide a novel and user-centric means of accessing digital systems and personal accounts. This approach aims to strike a balance between security and user convenience, offering a more engaging and intuitive method of proving one's identity while fortifying digital security.

By utilizing images, patterns, or other graphical components, users can create authentication credentials that are not only unique but also easier to remember, reducing the risk of forgotten passwords or insecure practices like password sharing. This method opens new possibilities for secure access across various digital platforms, from smartphones and tablets to computer systems and online accounts.

Graphical authentication combines the principles of security and usability, offering an exciting alternative to traditional text-based methods. This introduction sets the stage for exploring the world of graphical authentication, its advantages, challenges, and its potential to revolutionize the way we protect and access our digital identities in an ever-evolving digital landscape.

II. EXISTING AUTHENTICATION METHODS

A. Passfaces

Passfaces is a graphical password authentication system where users are required to recognize a pre-selected set of faces among a grid of other faces. Users typically set up their account by selecting a group of faces that are familiar to them. During authentication, they must identify their chosen faces from a randomized grid. This system aims to leverage human visual memory for authentication.

Memory Load: Users must remember a set of passfaces chosen during enrollment. Depending on the system's design, users may need to remember a considerable number of passfaces, which can increase cognitive load and the likelihood of forgetting chosen faces.

Vulnerability to Guessing Attacks: Passfaces may be susceptible to guessing attacks, where an attacker attempts to guess the user's passfaces by leveraging knowledge about the user's preferences or social engineering techniques. If the passfaces are based on publicly available information or easily deducible patterns, the system's security may be compromised.

User Familiarity with Faces: Users may have difficulty recognizing faces, particularly if the passfaces are unfamiliar or difficult to distinguish. This can lead to frustration and authentication failures, especially for users who have difficulty recognizing facial features or expressions.

B. DAS (Draw-a-Secret)

DAS (Draw-a-Secret): DAS is a system where users draw a shape or a pattern as their password. Unlike the Android pattern lock screen, DAS typically allows users to draw their shapes freely, rather than constraining them to a grid. Authentication is based on recognizing the drawn shape rather than its specific location.

Difficulty in Creating Complex Patterns: Users may find it challenging to create and remember complex drawing patterns. This limitation can lead to users choosing simplistic patterns that are easier to recall, potentially weakening the system's security against guessing attacks.

Vulnerability to Shoulder Surfing: Observers may be able to deduce the user's drawn pattern through visual observation, especially if the pattern is simple or repetitive. This vulnerability compromises the system's security, as attackers can potentially replicate the pattern to gain unauthorized access.

Accuracy of Pattern Recognition: DAS systems rely on accurately recognizing users' drawn patterns during authentication. However, factors such as variations in drawing speed, precision, or device sensitivity can affect the system's ability to accurately authenticate users, leading to false rejection or false acceptance errors.

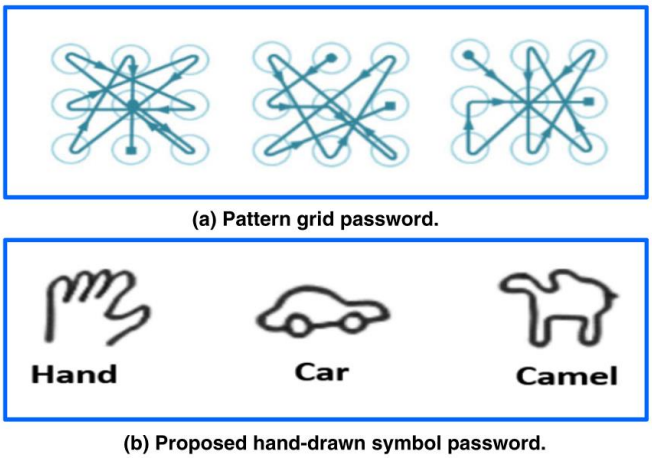
C. Token-based authentication

Token-based authentication involves the use of physical devices, such as security tokens or smart cards, to authenticate users. These devices generate one-time passwords (OTPs) or cryptographic keys that users must enter along with their regular credentials to access a system or service. Token-based authentication provides an additional layer of security, as the generated codes are typically time-sensitive or tied to the device itself.

Dependency on Physical Tokens: As mentioned earlier, token-based authentication relies on users possessing physical tokens. This introduces limitations such as the risk of token loss or theft. If a user forgets or loses their token, they may be unable to access the system until a replacement is issued.

Cost and Complexity: Implementing token-based authentication systems can be expensive and complex. The initial setup costs include purchasing tokens, configuring authentication infrastructure, and integrating token management systems. Additionally, managing a large number of tokens across distributed environments can pose logistical challenges.

Risk of Token Compromise: Physical tokens can be susceptible to theft, tampering, or duplication. If an attacker gains access to a user's token, they may be able to impersonate the user and gain unauthorized access to sensitive systems or resources.



(a) Pattern grid password.

(b) Proposed hand-drawn symbol password.

Fig.1: Existing Systems

III. GRAPHICAL PASSWORD STRATEGY AUTHENTICATION

Graphical authentication stands as an innovative approach to user identity verification, departing from traditional alphanumeric passwords and PINs. Instead, it leverages graphical elements, visual cues, or images to provide a novel and user-centric means of accessing digital systems and personal accounts. This approach aims to strike a balance between security and user convenience, offering a more engaging and intuitive method of proving one's identity while fortifying digital security.

By utilizing images, patterns, or other graphical components, users can create authentication credentials that are not only unique but also easier to remember, reducing the risk of forgotten passwords or insecure practices like password sharing. This method opens new possibilities for secure access across various digital platforms, from smartphones and tablets to computer systems and online accounts.

Graphical authentication combines the principles of security and usability, offering an exciting alternative to traditional text-based methods. This introduction sets the stage for exploring the world of graphical authentication, its advantages, challenges, and its potential to revolutionize the way we protect and access our digital identities in an ever-evolving digital landscape.

A. . Design Principles:

Drawing signature-based graphical passwords offer a unique approach to authentication by capitalizing on users' natural drawing abilities. The design principles underlying this authentication method aim to strike a balance between security and usability, ensuring that users can create authentication credentials that are both memorable and robust against attacks.

One of the key design considerations is the creation of a user-friendly interface for signature creation during the enrollment process. Users should be provided with intuitive drawing tools that allow them to express their unique drawing styles

effectively. The interface should offer flexibility in terms of the types of patterns or shapes users can create, accommodating a wide range of preferences and drawing abilities.

Grid layouts can be utilized to guide users in creating their signatures, offering a structured framework within which users can draw their patterns. However, the grid should not impose overly strict constraints that limit users' creativity or make it difficult for them to create meaningful signatures. Developers should explore different grid configurations and adapt them based on user feedback to strike the right balance between structure and flexibility.

Feedback mechanisms are essential for guiding users during the signature creation process. Real-time feedback, such as visual cues or auditory prompts, can help users refine their signatures and ensure that they meet the required complexity criteria. Additionally, informative error messages should be provided to users if their signatures do not meet the specified requirements, along with suggestions for improvement.

Security considerations are paramount in the design of drawing signature-based graphical passwords. To mitigate the risk of shoulder surfing attacks, developers should implement randomized grid layouts or dynamic challenge-response mechanisms that require users to replicate a specific pattern or shape within a predefined timeframe. Furthermore, the system should employ techniques such as image distortion or encryption to protect users' signatures from interception or tampering.

Overall, the design of drawing signature-based graphical passwords should prioritize usability without compromising security. By providing users with intuitive drawing tools, structured guidance, and effective feedback mechanisms, developers can empower users to create authentication credentials that are both memorable and resilient against attacks.

B. Implementation Strategies:

Implementing drawing signature-based graphical passwords requires the integration of user interface components for signature creation, storage, and authentication within the target system. This section explores various implementation strategies and technologies that can be employed to realize the functionality of drawing signature-based authentication.

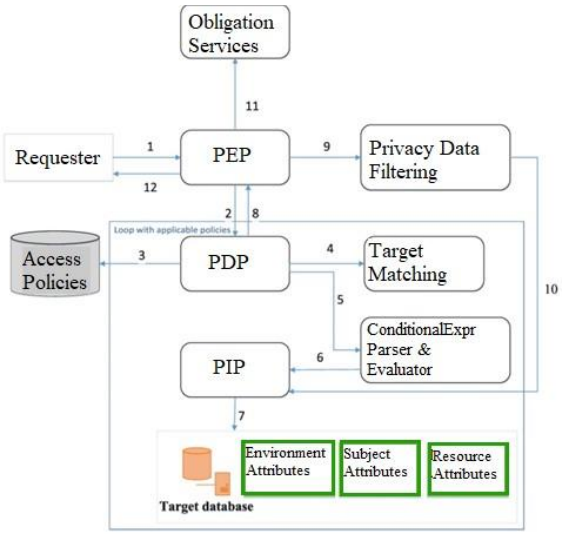


Fig.2: Implementation Strategy

C. User Interface Design:

The user interface for signature creation plays a crucial role in the usability of drawing signature-based graphical passwords. Developers should design intuitive and responsive interfaces that allow users to draw their signatures easily and accurately. This may involve implementing drawing tools such as brushes, pens, or styluses, along with features such as undo/redo functionality and zoom capabilities to facilitate precise drawing.

Grid Layouts and Feedback Mechanisms:
Grid layouts can provide users with a structured framework for creating their signatures, helping to ensure consistency and accuracy. Developers should design grid layouts that strike a balance between providing guidance and allowing for creativity. Additionally, real-time feedback mechanisms can be implemented to provide users with immediate feedback on the quality and complexity of their signatures, helping them to refine their creations.

Signature Storage and Authentication:
Once users have created their signatures, the system must securely store and authenticate them during the login process. Signatures can be stored as digital representations, such as image files or vector graphics, in a secure database or file system. During authentication, users' drawn signatures are compared against their stored counterparts using algorithms for signature recognition and verification.

Technologies and Algorithms:
Several technologies and algorithms can be leveraged to implement drawing signature-based graphical passwords effectively. Digital signature recognition algorithms, such as machine learning models or pattern recognition algorithms, can be used to analyze and verify users' drawn signatures. Additionally, encryption and hashing techniques can be employed to protect users' signatures from unauthorized access or tampering.

Integration and Compatibility:
Drawing signature-based graphical passwords must be seamlessly integrated into existing authentication systems and compatible with various devices and platforms. Developers should ensure that the implementation supports cross-platform compatibility, allowing users to create and authenticate their signatures on desktop computers, tablets, smartphones, and other devices.

Usability Implications:

Drawing signature-based graphical passwords offer several usability advantages over traditional alphanumeric passwords, but they also present unique challenges and considerations that must be addressed to ensure a positive user experience.

D. Advantages:

One of the primary advantages of drawing signature-based graphical passwords is their inherent memorability. Users tend to find it easier to remember visual patterns or shapes compared to complex alphanumeric strings, leading to a reduction in forgotten passwords and password reset requests. Additionally, drawing signatures allow users to express their creativity and individuality, enhancing the personalization and user engagement of the authentication process.

IV. SYSTEM ARCHITECTURE AND ALGORITHMS

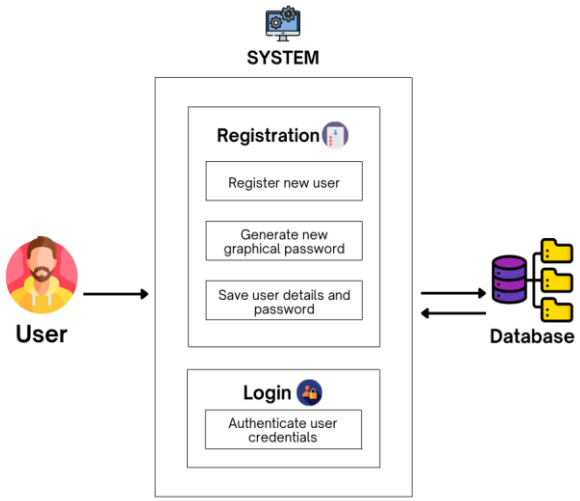


Fig.3: Graphical Authentication System

In the domain of Graphical Password Strategy Authentication, a range of algorithms play a pivotal role in ensuring robust security and user-friendly authentication methods. Below are some of the commonly employed algorithms tailored to this purpose:

A. Visual Cryptography:

Visual Cryptography is a cryptographic technique specifically designed for graphical password systems. It takes advantage of images or patterns as secret keys and uses visual sharing schemes to enhance security. With Visual Cryptography, an image is divided into multiple shares, and by stacking these shares together, the original image, or password, is revealed. This technique aligns perfectly with the graphical nature of passwords and offers a strong layer of protection.

B. **Pattern Recognition with Neural Networks:**

Pattern recognition, especially using neural networks, proves highly effective in the graphical password authentication context. Neural networks can be trained to recognize specific patterns or images,

ensuring that the authentication process is not only secure but also responsive to user input. By adapting to user behavior and preferences, these networks create a dynamic and adaptive authentication experience.

C. Cognitive Biometrics:

Cognitive biometrics is a cutting-edge approach in the field of graphical password authentication. It leverages user-specific cognitive traits and behaviors, such as how a person draws or interacts with graphical elements, to create highly personalized and secure authentication systems. These traits are challenging for unauthorized users to mimic, making cognitive biometrics a promising avenue for enhancing security.

D. Machine Learning for Anomaly Detection:

Machine learning algorithms for anomaly detection are vital for identifying unusual behavior during graphical password input. By monitoring patterns and deviations in user interactions with graphical passwords, these algorithms can swiftly detect potential security threats or unauthorized access attempts. This proactive approach adds an extra layer of security to the authentication process.

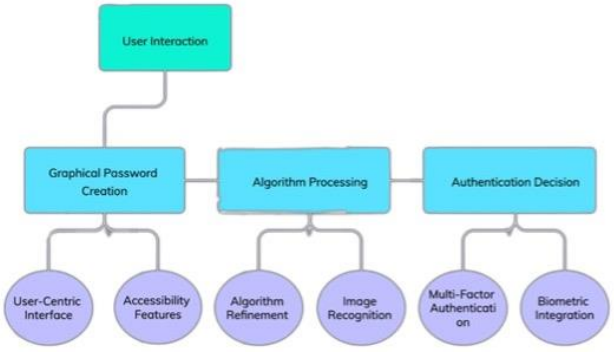


Fig.4: Graphical Authentication Architecture

V. APPLICATIONS

Applications of graphical password authentication in various fields:

1. **Healthcare**:

Electronic Health Record (EHR) Systems: Graphical password authentication can secure access to patient records, ensuring that only authorized healthcare professionals can view sensitive medical information.
Prescription Management Platforms: Healthcare providers may use graphical passwords to access systems for managing prescriptions and medication orders securely.

2. **Education**:

Online Learning Platforms: Graphical password authentication can be used for student and instructor logins to access course materials, participate in discussions, and submit assignments securely.
Student Information Systems: Educational institutions may implement graphical passwords to protect student data in systems for enrollment, grading, and academic records.

3. **Finance**:

Online Banking: Graphical password authentication provides an additional layer of security for accessing bank accounts, transferring funds, and performing financial transactions on banking websites and mobile apps.
Trading Platforms: Stock trading and investment platforms may utilize graphical passwords to authenticate users and protect sensitive financial data.

4. **Government**:

Secure Portals: Government agencies may use graphical passwords to control access to secure portals for accessing government services, filing taxes, and submitting official documents securely.
Law Enforcement Systems: Graphical password authentication can secure access to databases and systems used by law enforcement agencies for criminal investigations and record-keeping.

5. **Retail**:

Point-of-Sale (POS) Systems: Retailers may implement graphical password authentication for accessing POS

systems, managing inventory, and processing sales transactions securely.
E-commerce Platforms: Online retailers can use graphical passwords to authenticate users and protect customer accounts, order history, and payment information on e-commerce websites.

6. **Research**:

Scientific Data Repositories: Research institutions may employ graphical password authentication to secure access to databases and repositories containing scientific data, research findings, and experimental results.
Collaboration Platforms: Graphical passwords can safeguard collaboration platforms used by researchers to share data, collaborate on projects, and communicate securely.

7. **Entertainment**:

Streaming Services: Video streaming platforms may utilize graphical passwords to authenticate users and protect access to subscription-based content libraries, personalized playlists, and viewing history.
Gaming Accounts: Online gaming platforms can use graphical passwords to secure player accounts, in-game purchases, and virtual assets in multiplayer games and gaming communities.

8. **Transportation**:

Fleet Management Systems: Transportation companies may implement graphical password authentication for accessing systems used to manage vehicle fleets, track shipments, and optimize logistics operations securely.
Passenger Booking Portals: Airlines and public transportation providers can use graphical passwords to authenticate users and protect passenger booking information, travel itineraries, and loyalty program accounts.

VI. CHALLENGES

Implementing drawing signature-based graphical passwords introduces both opportunities and challenges in the realm of authentication.

One of the primary challenges is ensuring the accessibility of the authentication method for users with disabilities. Users with motor impairments or visual impairments may face difficulties in creating and interacting with drawn signatures.
Addressing this challenge requires implementing accessibility features such as alternative input methods, voice commands, or screen reader support. Ensuring inclusivity and accessibility for all users is essential for the widespread adoption and effectiveness of drawing signature-based authentication systems.

VII. CONCLUSION

Drawing signature-based graphical passwords offer a novel approach to authentication that leverages users' natural drawing abilities to create memorable and secure authentication credentials. By incorporating design principles, implementation strategies, usability considerations, and security best practices, developers can create drawing signature-based authentication systems that offer both enhanced security and user experience. However, further research is needed to address the challenges and vulnerabilities associated with this authentication method, and to refine the design and implementation to ensure its effectiveness and usability in real-world scenarios. With continued innovation and refinement, drawing signature-based graphical passwords have the potential to become a widely adopted authentication mechanism, offering a compelling alternative to traditional alphanumeric passwords and enhancing the security and usability of digital systems.

VIII. REFERENCES

[1]. Dhamija, R., & Perrig, A. (2000). Déjà vu: A user study using images for authentication. In Proceedings of the 9th conference on USENIX Security Symposium (Vol. 9, pp. 1-15).

[2]. Thorpe, J., & Thorpe, M. (2008). Graphical passwords: A survey of usability issues. In Proceedings of the Fourth Symposium on Usable Privacy and Security (SOUPS 2008) (pp. 1-12).

[3]. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12).

[4]. Vishwanath, A., & Dhamija, R. (2007). PassPoints: design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 65(12), 965-984.

[5]. Monrose, F., & Reiter, M. K. (1999). Memorability and security: risk assessment of graphical passwords. In International Workshop on Security Protocols (pp. 1-15). Springer, Berlin, Heidelberg.

[6]. Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 1-38.

[7]. Dunphy, P., & Yan, J. (2011). A new framework for graphical password protection based on cued-recall. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec'11) (pp. 9-16).

[8]. Vidyaratne, L., Samarasekera, S., & Wijayarathna, G. (2009). Enhanced graphical password authentication using perspective distortion. In 2009 International Conference on Industrial and Information Systems (pp. 121-126). IEEE.

[9]. Uzun, E., & Furnell, S. (2008). A survey of user authentication based on graphical passwords. The Journal of Systems and Software, 81(9), 1489-1511.

[10]. De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(1-2), 128-152.

[11]. Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 1-38.

[12]. Akakpo, C. A., Belenkiy, M., Bellovin, S. M., Keromytis, A. D., & Reiter, M. K. (2009). KittenAuth: a new graphical authentication system. In Proceedings of the 2009 workshop on New security paradigms (pp. 37-48).

[13]. Tari, F., & Ozok, A. A. (2006). Graphical authentication and virtual reality: A case study with dynamic security skins. In International Conference on Universal Access in Human-Computer Interaction (pp. 746-755). Springer, Berlin, Heidelberg.

[14]. Gu, J., Zhu, S., & Zou, C. C. (2021). Graphical Password-based Authentication System with Improved Usability and Security. IEEE Transactions on Dependable and Secure Computing.