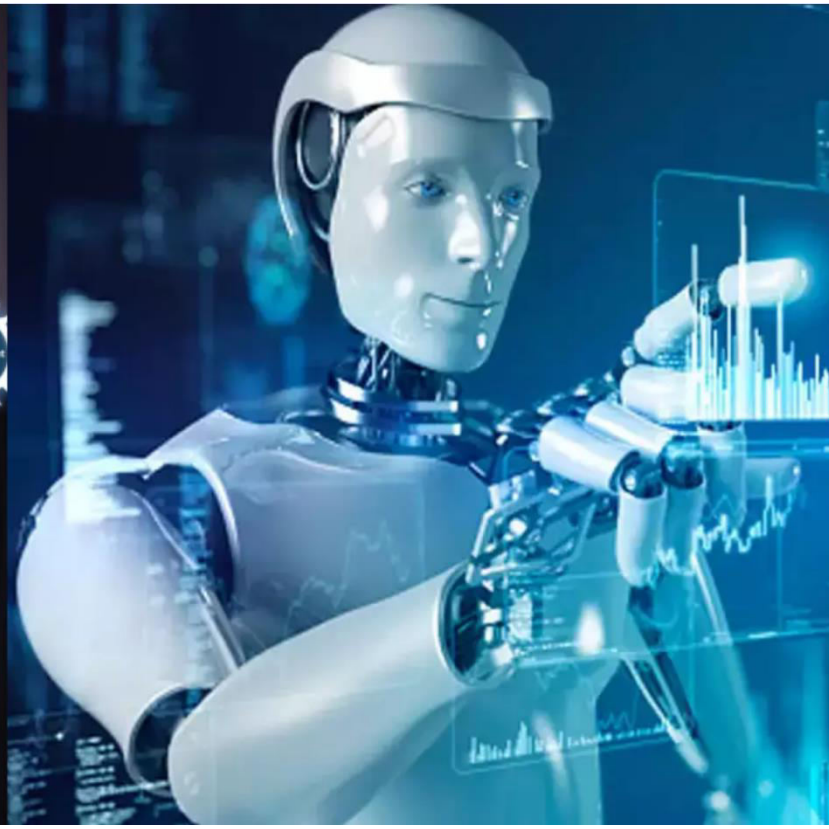
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

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

Impact Factor 8.699

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

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412070|

Graphical Password with Pass Points and Secure Resource Repository for Authorized users

Dumbika T P[1], Ajith G L[2]

Student, Dept. of MCA, PES Institute of Technology and Management, Shivamogga, Karnataka, India[1]

Assistant Professor, Dept. of MCA, PES Institute of Technology and Management, Shivamogga, Karnataka, India[2]

ABSTRACT: The new class of passwords that replace the conventional alphanumeric passwords is known as graphical passwords. They are intended to make security much safer and more user-friendly. The Pass Points method a graphical login system that requires clicking will be examined in this research paper along with how it functions in conjunction with a user-authorized secure file store. The idea is that images are easier for people to remember than words. This makes passwords easier to use and enables users to create stronger passwords. One of the most important parts of the system is the Pixel Tolerance Calculation. It enables people to click off a little while maintaining the security of their login.

KEYWORDS: Graphical Password Authentication, Pass Points Scheme, Click-based Authentication, Pixel Tolerance Calculation, Secure Resource Repository, Image-based Passwords, Human Visual Memory, Usability and Security, Authentication Mechanism, Encrypted Password Storage, Shoulder-Surfing Resistance, Brute Force Attack Resistance, User-Friendly Authentication, Secure Access Control, Memorability of Passwords.

I. INTRODUCTION

Digital security has changed since standard alpha-numeric passwords are no longer adequate. These text passwords which were once thought to be sufficient to keep hackers out are now susceptible to advanced hacking techniques like phishing and brute-force. They are often referred to as the weakest link in the chain because humans who use them account for a large part of the issue. Users are required to create and pass a lot of complicated passwords which makes them hard to remember and encourages insecure practices like using simple passwords or not changing them at all. Because of this security researchers are turning their attention to graphical password systems which use the brains superior memory for pictures and other visual patterns instead of letters and numbers. In this paper, the author discusses the Pass Points system which is a widely used system of picture passwords that are click-based and in which a user logs in by selecting a particular set of points on a picture. As a result keypad passwords are easier to remember more convenient through visual memory and less likely to be lost due to keylogging. However the picture password systems could still be compromised by shoulder-surfing. This suggests that a thorough examination is required to ascertain their level of safety and usefulness while also proposing a plan of action for their implementation in a reliable secure resource library thereby simplifying and enhancing the login process..

II. LITERATURE SURVEY

Dasgupta, Roy, and Nag [1] suggested a set of graphical passwords that are both secure and easy to use through an intuitive interface. They also contend that by using this method the likelihood of password guessing will be significantly reduced which will completely deter attackers. Adaptive techniques are said to be able to strengthen the system without sacrificing the user experience.

Chiasson, van Oorschot, and Biddle [2] found that the password area created by the prompted images and user recall are better than those created by the previous text-based passwords making them more resistant to guessing and brute force attacks.

Sobrado and Birget [3] suggest challenge-response strategies which have also led to additional advancements in the field of graphic passwords. Others in the field who have dealt with coarse-grained solutions to issues pertaining to the monotony of alphanumeric passwords have those based on their research

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

Impact Factor 8.699

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

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412070|

Wiedenbeck, Waters, Birget, Brodskiy, and Memon [4] Each user is given a password consisting of a few markers on a single image in this arrangement. Their long-term studies have confirmed the publics capacity to recall these cues over time and the frequency of their occurrence.

Suo, Zhu, and Owen [5] categorized graphical password systems into recognition-based recall-based and hybrid approaches in order to study the technique. They compared the two approaches and looked at their advantages disadvantages and security risks. that has since been used in numerous studies on graphical authentication.

Mishra, Jadhav as well as Patil [6] developed a graphical password system. This is a significant problem with graphical logins usability. In order to protect the password even when someone is watching the sign-in their design relies on arbitrary choices and visual tricks.

Gurav, Gawade, Rane, and Khochare [7], cloud storage and trustworthy authentication. They direct their efforts toward the security of information in distributed environments and demonstrate that employing graphical..

Adamu, Mohammed, Adepoju, and Aderiike [8] proposed a three-step hybrid log-in system that includes picture text and one-time passwords Their system ensures security is safer as various protection means are stacked, the weakness in one specific method is lowered and is user friendly.

III. PROPOSED METHODOLOGY

Strong access controls a secure backend and a graphic password system are all used in this system to guarantee security. The user chooses a background image on the front end then clicks a series of points on the image to create a password. The system uses a Pixel Tolerance Calculation which determines a small acceptable area around each point of the chosen point because humans dont always click at the exact same spot. In order to identify predictable or non-random passwords the pattern of points is validated during registration using a test called a mean distances test. This guarantees that the system is more secure even at the outset. The same password works with different screen sizes and display resolutions because the system also uses the click coordinates as the relative points.

The suggested approach uses a layered approach to provide high security. Every time you try to log in the system will randomly rotate the picture pieces to prevent people from seeing what you log in—a significant annoyance with fixed picture passwords. No real passwords will be kept in plaintext since the users encrypted position and information will be securely stored in the database using a robust hash like SHA-256. This image-based identifiable will also be integrated with a multi-factor authentication whereby a second step such as a one-time password will be part of it. A powerful permissions system will restrict access to other users to what they may see and do in the safe resource space, thus they will only access the data access is granted.

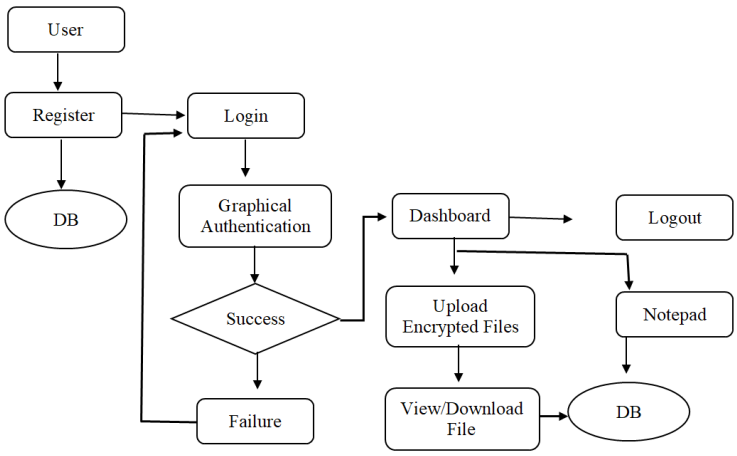


Fig. 1: Data Flow Diagram

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

Impact Factor 8.699

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

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412070|

When a user interacts with the secure graphical authentication system this DFD depicts the entire process. When a new user registers by entering their information and choosing their graphical password the process starts. After being safely encrypted these details are kept in the database. The user must replicate their selected click-points on the image during the graphical authentication step when they later try to log in. The system allows access and directs the user to their dashboard if the click sequence matches the stored pattern. They are sent back for another attempt at login if the authentication is unsuccessful. After entering the dashboard users can safely upload files which are instantly encrypted before being stored. Additionally the system decrypts the data only for authorized access allowing users to view or download previously uploaded files. Users can also safely store text in the database thanks to an integrated notepad feature. Anytime the user wants to safely end the session they can log out. All things considered this flow guarantees that every stage from file handling to registration is safeguarded with encryption and stringent authentication offering a seamless and safe user experience.

Algorithms Used:

The project relies on two powerful yet easy-to-understand algorithms that work together to provide both secure login and safe data handling. First it employs the Pass Point Scheme a graphical authentication technique that eliminates the need for complicated passwords by having users click on memorable locations within an image. Because each persons exact click points are different and challenging for an attacker to figure out this makes login feel more natural and user-friendly while maintaining strong security. The AES (Fernet) Encryption Algorithm which converts sensitive data into unintelligible code that can only be decrypted with a unique key is used by the system to secure the users files and text after they have been verified. This guarantees that even if someone manages to access the stored data they wont be able to decipher or utilize it improperly. When combined these algorithms provide a seamless secure experience that enables users to confidently store their data and log in visually.

1. Pass Point Scheme Algorithm (Graphical Authentication): By clicking on particular points within an image users can create a password using the Pass Point Scheme a graphical password method. The user chooses multiple memorable locations such as a buildings corner a distinctive shape or a recognizable object within a single background image in place of typing characters as in traditional passwords. The user does not need to click the precise pixel during login because the system records the precise coordinates of each click during registration with some tolerance. The user has to click on those same points in the right order when logging in. The system deems the clicks to be a match and allows access if they are within the permitted tolerance range. Because it introduces a large password space and makes it difficult for attackers to guess personal click-locations simply by looking this method is more secure against dictionary and brute-force attacks. Since people frequently remember pictures and visual cues better than lengthy text passwords the algorithm also improves usability. Overall by making authentication a natural visual interaction the Pass Point Scheme achieves a balance between security and user-friendliness.

2. AES (Fernet) Encryption Algorithm (File & Text Security): The project uses the AES (Fernet) encryption algorithm to safely encrypt and decrypt user-inputted text and sensitive files. Fernet is essentially a cryptographic implementation that ensures data integrity and confidentiality by using AES-128 in CBC mode and HMAC for authentication. When a user uploads a file or enters text the system creates a unique key and encrypts the data turning it into ciphertext that is unintelligible to anyone who does not have the matching key. Even if someone manages to get access to the stored file this prevents data from being stolen leaked or altered. In order to stop the misuse of outdated or expired encrypted content Fernet also timestamps encrypted data. The system uses the same key to decrypt a file back into readable form when the user downloads or views it. Because it manages both encryption and verification in a single step this algorithm is widely trusted in contemporary security systems. It is straightforward but extremely secure. To put it briefly AES (Fernet) guarantees that the users text and files are protected throughout the entire application process.

Software Testing:

System testing is like giving your entire project a final check-up to ensure everything works together as it should. It's the stage where the whole application user interface, algorithms, database, encryption, and all features comes together and is tested as one complete system. Instead of checking small pieces individually, system testing focuses on how those pieces behave when they interact. It helps you see the application the same way a real user would, ensuring that the login process is smooth, encryption works flawlessly, and all screens respond correctly. In short, system testing helps confirm that the project is ready for real-world use without surprises or hidden issues.

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

Impact Factor 8.699

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

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412070|

1. Unit Testing Unit testing is like checking each small ingredient before cooking the final dish. Every tiny part of the project such as the function that encrypts data, the code that saves click points, or the method that matches authentication coordinates is tested separately. This ensures that each component works perfectly on its own, reducing future errors and making the system more reliable.

2. Integration testing makes sure that different modules of the system can communicate smoothly. It checks how the login page works with the graphical password module, how encryption interacts with file upload, and how the database responds to user actions. It's like seeing whether the gears in a machine rotate together without jamming or slipping.

3. Functional Testing Functional testing focuses on the question of whether the system functions as intended. Creating new users selecting password hints logging in encrypting files and other tasks are all carried out by testers. text decryption. Like checking a to-do list it ensures that every function specified in the requirements is operational. items that were missed.

4. Usability testing evaluates the systems perceived friendliness and usability. It confirms that the user does not feel confused the process is coherent and the icons are intuitive. exhausted when it was all over. Its similar to letting someone use your app and then monitoring whether they get lost or navigate through it without any problems.

5. Security testing identifies any possible threats to an attackers attempt to access the system it verifies that click- point passwords can't be guessed easily, encrypted data stays protected, and no unauthorized user can sneak into the system.

6. Performance Testing In essence performance testing ascertains how the system behaves when executing multiple tasks or engaging with multiple users. Large file uploads dont cause the application to lag encryption doesn't add any waiting times and it instantly confirms that users are logged in.

7. Compatibility Testing Compatibility testing ensures that the system operates consistently across various devices screen resolutions and browser types. It examines whether the program works well and is aesthetically pleasing on PCs smartphones and browsers like Google Chrome Firefox or Edge.

8. System testing verifies that the application functions as a whole with the database Flask backend AES encryption and graphical password system all functioning flawlessly employment.

9. UAT is the final method of user interaction. It is now up to the actual users or testers to verify that the system functions as intended. The project can be deployed if users are satisfied and everything is operating as it should. It is comparable to receiving a last-minute approval.

IV. EXPERIMENTAL RESULTS

The experimental results show that the system performs reliably, allowing users to register and authenticate using graphical click-points with high accuracy. AES (Fernet) encryption successfully protected all stored files and password data, ensuring that no sensitive information was exposed during testing. Users found the graphical login process easier to remember compared to traditional text passwords, resulting in fewer login errors. Overall, the tests confirm that the system is both secure and user-friendly in real-world usage.

Home Page

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

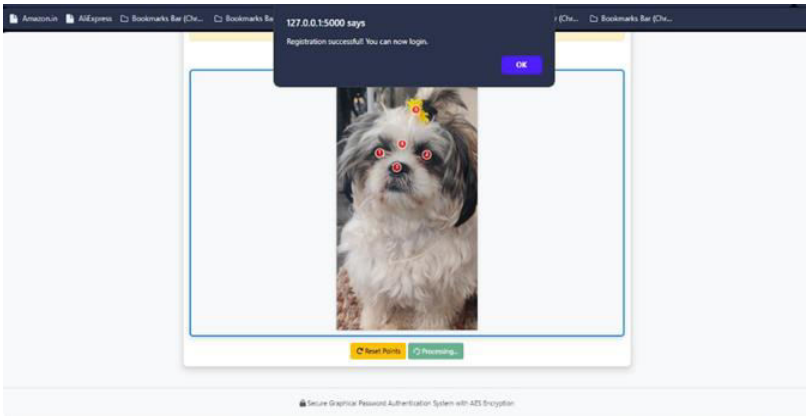
Impact Factor 8.699

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

Volume 14, Issue 12, December 2025

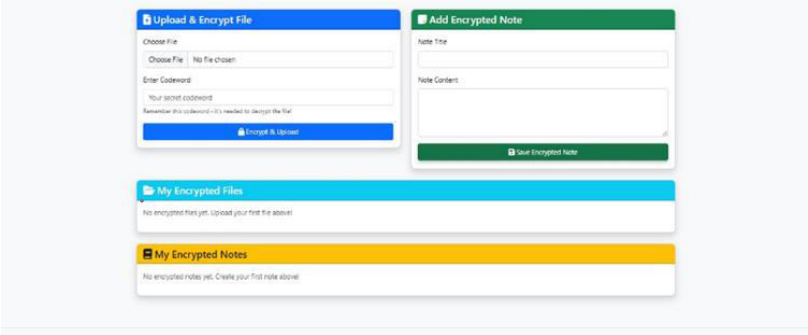
|DOI: 10.15680/IJIRSET.2025.1412070|

This image shows the homepage of a Graphical Password Authentication System, presented with a clean and modern interface. At the top, there is a blue navigation bar with links for Home, Login, and Register, making it easy for users to move around the system. The main section features a centered card with a shield icon, emphasizing security and trust. Below the title, the system highlights its purpose providing strong protection using Pass Point Scheme and AES Encryption.



Pass Point Selection Page

This image shows the point-selection step of the graphical password setup process. The user has uploaded a picture of a dog and selected five secret click points, which are marked with red indicators on the image. A pop-up message at the top confirms that the registration was successful and the user can now proceed to login. Below the image, options like Reset Points and Processing… guide the user through finalizing their selection.



User Dashboard Page

This image shows the main dashboard of the Graphical Auth System after the user logs in. The interface provides two main options: uploading and encrypting a file, or creating an encrypted note. Below these panels, sections for encrypted files and notes appear, both currently empty. The layout is clean and guides the user toward securely storing their files and text.

V. CONCLUSION

This project shows how combining AES (Fernet) encryption with the Pass Point graphical password method can make a login system more secure and user-friendly. Instead of having to remember lengthy or complicated text passwords users only need to choose particular points on an image which is more memorable and feels more natural. To prevent unwanted access all user data and the click-points they choose are encrypted. As a result the entire authentication process is both user-friendly and safe thanks to these features. In summary this system eliminates the typical issues with conventional password methods and provides a good balance between safety and convenience. While lowering the

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

Impact Factor 8.699

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

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412070|

vulnerabilities to shoulder surfing bruteforce attacks and basic password guessing it encourages users to engage with the authentication process. The projects functionality and modularity are strong and it fortifies the roadmap for future advancements like adaptive security features real-time intrusion detection and multi-image authentication. In the end it demonstrates that security doesnt have to be difficult it can be breathtaking alluring and very effective.

REFERENCES

[1] "Toward the design of adaptive selection strategies for graphical password authentication" by Dasgupta, D, Roy, A, & Nag, A.
[2] "Graphical password authentication using cued click points" by Chiasson, S, van Oorschot, P. C, & Biddle, R.
[3] "Graphical passwords. In Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks" by Sobrado, L., & Birget, J. C.
[4] "Pass Points: Design and longitudinal evaluation of a graphical password system" by Wiedenbeck S, Waters J., Birget J. C, Brodskiy A, & Memon N.
[5] "Public Graphical passwords: A survey. In 21st Annual Computer Security Applications Conference" by Suo X, Zhu Y, & Owen G. S.
[6] "A Shoulder-Surfing Resistant Graphical Password System" by Aditya Mishra, Rahul Jadhav, Shubham Patil.
[7] "Graphical Password Authentication: Cloud Securing Scheme" by Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare.
[8] "A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication" by Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju, Abisoye Opeyemi Aderiike.
[9] "Graphical Password Authentication: Cloud Securing Scheme" by J. D. Jain, A. H. Khan, A. K. Jain, and M. R. P. D. S.
[10] "A paper combining graphical passwords and One-Time Passwords (OTPs)" by M. Sreelatha.
[11] "Graphical Password Authentication" from the International Advanced Research Journal in Science, Engineering and Technology.
[12] "Graphical password authentication system using Cued Click Points" by S. Wiedenbeck, E. B. B. B. J., S. S., & P. B.
[13] "A paper detailing the Pixel Tolerance Calculation" in a graphical password system from JETIR.
[14] "New Test to Detect Clustered Graphical Passwords in Passpoints Based on the Perimeter of the Convex Hull" from MDPI.
[15] "On User Choice in Graphical Password Schemes" by M. K. Reiter, M. E. Greenstein, S. R. B. H., & R. L.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details