Gurukul International Multidisciplinary Research Journal (GIMRJ)*with*
International Impact Factor 8.249
Peer Reviewed Journal
https://doi.org/10.69758/WNPQ6244

e-ISSN No. 2394-8426
Special Issue On Advanced Computational Techniques: Emerging Trends from Postgraduate Studies
Issue–I(VI), Volume–XII

TRIUMPH OF SECURITY : FORTIFYING DIGITAL FORTRESSES WITH TRIPLE GUARD AUTHENTICATION

Miss Apurva Pradip Dhamange
PG Scholar
Department of Computer Science
G H Raisoni University Amravati , India

Received on: *11 April ,2024* ***Revised on:*** *26 May ,2024,* ***Published on:*** *01 June ,2024*

Abstract : Network security is crucial in today's interconnected world, and traditional text-based passwords are insufficient. This paper introduces a Three-Level Security system to enhance protection with a multi-tiered approach: Level-1 Login-based Password, Level-2 Graphical Authentication, and Level-3 Image-Based Password. The system ensures authorized access, defines user permissions, and encrypts data. It includes monitoring, rate limiting, regular updates, and penetration testing, using Python-based tools for vulnerability scanning. Triple Guard encrypts data both at rest and in transit, ensuring confidentiality and integrity.

It adaptive to emerging threats and vulnerabilities, integrating Python-based security testing tools for vulnerability scanning and code analysis. By providing developers and administrators with a robust and extensible password security solution . Triple Guard encrypts data both at rest and in transit, preserving its confidentiality and integrity.

Index Terms :-. Login Password Authentication, Graphical Authentication, Image Authentication, Python, Chatgpt.

I. INTRODUCTION

Security plays major role in every network system which we use in our day to day life. Triple Guard provides a holistic approach to security, addressing vulnerabilities across multiple layers of threats. , Triple Guard encrypts data both at rest and in transit, preserving its confidentiality and integrity. Our project, a Three-Level Password System using Python, aims to enhance security by incorporating three levels of authentication – Textual, Image, and Graphical. python-based Three-Level Password System is designed to overcome the problem. It is an authentication system that only allows users to access the system if they have entered the correct password. The project includes three levels of user authentication – Textual, Image and Graphical. That way there would be negligible chances of the bot or anyone else cracking the passwords, even if they crack the first or second level it would be impossible to crack the third. It emphasizes the need for multi-layered protection to safeguard sensitive information and prevent Unauthorized security . Triple Guard's ability to safeguard critical data assets against internal and external threats. Creating a graphical security system for authentication can enhance the user experience and security of a login system. Triple Guard encrypts data both at rest and in transit, preserving its confidentiality and integrity. Granular access controls, data masking techniques, and data loss prevention (DLP) measures further enhance Triple Guard's ability to safeguard critical data assets against internal and external threats. Authentication and security are two terms which are interrelated. Authentication is the act of confirming the exactness of an attribute of a distinct piece of data (datum) or entity.for any type of applications, sites, etc. In this system, users can first register in the system and after the registration

process; the users can login to It is actually the process of confirming the identity. It is an application that is generally intended for providing security the system using the same details they provided during the registration. As this system has 3 levels of security, any intruder will not be able to hack the details of the users. The key distinction between security and responsibility is that security should take under consideration the actions of individuals making an attempt to cause destruction.Here's a speculative breakdown of potential objectives for such a framework:The system is user-friendly and has simple interface. Provides strong security against bot attacks or hackers. Users can set or upload their own images. .Protects systems vulnerable to attacks. The project is an authentication system that validates user for accessing the system only when they have input correct password .The project involves three levels of user authentication.

II. RELATED WORK

The main Objective of 3-Level Security system is a unique and an esoteric study of using images as password which helps to give extreme secure to the system, thus we are employing 3 levels of security

Text Authentication (LEVEL-1)

Graphical Authentication (LEVEL-2)

Image Authentication (LEVEL-3)

Static password is the traditional password which is usually changed only when it is necessary: it is changed when the user has to reset the password, i.e., either the user has forgotten the password or the password has expired. While dynamic password, also known as One Time Password (OTP), is a password which changes every time the user logs in. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Moreover, the first level employsthe static password due to the complexity of the One Time Password (OTP).Passwords have been used with computers since the earliest time of computing. This was introduced in 1961. It had a LOGIN command that requests a user password. After typing PASSWORD, the system turns off the printing mechanism, if possible, so that the user may type in his password with privacy. To log in, the user is asked to type the password which already given while creating login. Therefore, security at LEVEL1 is ensured by use of text password they are allowed to have special character which is a usual approach with normal login scheme photo. The concept of defense-in-depth involves implementing multiple layers of security controls throughout an organization's IT infrastructure. This approach aims to mitigate risks by incorporating various security measures, such as firewalls, intrusion detection systems, access controls, encryption, and security monitoring. Each layer of defense adds another obstacle for attackers to overcome, making it more challenging to penetrate the network and access sensitive information.

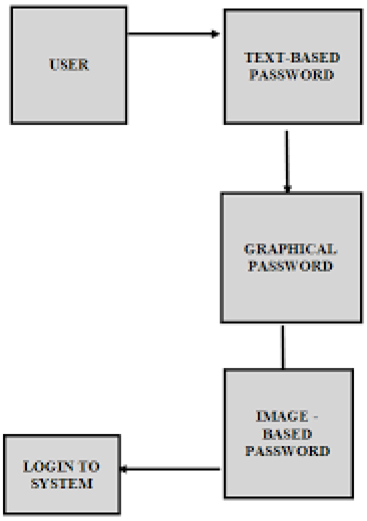


Fig 1: framework of study

Multi-Factor Authentication (MFA) stands out as a prominent approach, demanding users provide multiple forms of identification before access is granted. Complementary to this are password managers, facilitating the generation and storage of complex passwords across various accounts securely.Passwords have been used with computers since the earliest time of computing. This was introduced in 1961. It had a LOGIN command that requests a user password. After typing PASSWORD, the system turns off the printing mechanism, if possible, so that the user may type in his password with privacy. To log in, the user is asked to type the password which already given while creating login. Therefore, security at LEVEL1 is ensured by use password they are allowed to have special character which is a usual approach with normal login scheme photo.

Text representation of passwords encompasses various methods for encoding passwords as strings of alphanumeric characters or symbols. Traditional alphanumeric passwords, comprising a combination of letters, numbers, and special characters, remain ubiquitous.Keyboard patterns utilize the layout of a keyboard to create passwords based on typed characters forming a pattern. Leet Speak, a form of online jargon, substitutes characters with similar-looking symbols or numbers. Each method presents distinct trade-offs between security and memorability, emphasizing.

The importance of selecting a password strategy that aligns with individual preferences and security requirements while adhering to best practices for creating strong passwords.Graphical Passwords: Graphical passwords replace traditional alphanumeric passwords with images, patterns, or symbols. Passpoints require users to select specific points on an image, while draw-based systems prompt users to draw a pattern or gesture on a grid. Click-based methods involve clicking on predefined areas within an image. Recognition-based systems require users to identify or recognize specific images from a set of options. These graphical approaches offer an intuitive and potentially more memorable alternative to text-based passwords.Passfaces: Passfaces is a graphical authentication system that uses human faces as passwords. Users select a set of faces from a grid of images during enrollment and then identify those faces during login.Passfaces leverages the brain's innate ability to recognize faces, making it a user-friendly authentication method. first level, physical security, focuses on safeguarding the hardware and infrastructure through measures like secure access control systems, surveillance cameras, and environmental controls such as fire suppression and climate control systems. The second level, network security, aims to protect the network infrastructure from unauthorized access and attacks by employing firewalls, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), network segmentation, and data encryption during transmission.

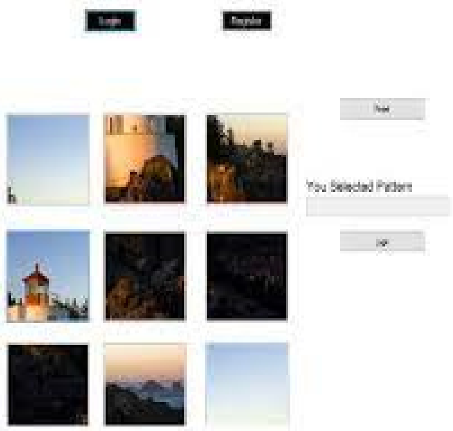


fig 3. screenshot of image password generator

These biometric authentication methods utilize images of the user's unique physiological features to verify their identity and grant access to the device or specific applications . This includes the use of firewalls to filter traffic, intrusion detection and prevention systems (IDPS) to monitor and respond to suspicious activities, virtual private networks (VPNs) for secure remote access, network segmentation to restrict access to sensitive information, and encryption to secure data in transit.

users must provide an image-based password, which could involve recognizing and selecting pre-chosen images from a set. This multi-tiered graphical representation not only ensures robust security by verifying identities through diverse methods but also enhances user engagement and ease of use. By visualizing the authentication process, it clearly demonstrates how each layer contributes to a fortified security system, ensuring that only authorized individuals gain access while maintaining a user-friendly interface.**Passfaces:** Passfaces is a graphical authentication system that uses human faces as passwords. Users select a set of faces from a grid of images during enrollment and then identify those faces during login. Passfaces leverages the brain's innate ability to recognize faces, making it a user-friendly authentication method.Image-Based CAPTCHAs: CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) often use images to challenge users and differentiate between humans and automated bots. Image-based CAPTCHAs may require users to identify objects, animals, or characters within an image to prove their human identity. A three-level security-based system involves implementing multiple layers of protection to ensure comprehensive defense against potential threats. The first level, physical security, focuses on safeguarding the hardware and infrastructure through measures like secure access control systems, surveillance cameras, and environmental controls such as fire suppression and climate control systems. The second level, network security, aims to protect the network infrastructure from unauthorized access and attacks by employing firewalls, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), network segmentation, and data encryption during transmission. The third level, application and data security, is centered on securing applications and sensitive data within the network. This includes the use of multi-factor authentication (MFA) and role-based access control (RBAC) to manage user access, implementing secure coding practices to prevent vulnerabilities, encrypting data at rest, maintaining regular updates and patch management, and deploying Security Information and Event Management (SIEM) systems to monitor and analyze security data for detecting and responding to threats. By integrating these layers, the system ensures that if one layer is compromised, additional layers continue to provide protection, creating a robust security posture.

Image-Based Authentication in Mobile Devices: Many mobile devices offer image-based authentication methods, such as fingerprint recognition, facial recognition, or iris scanning. These biometric authentication methods utilize images of the user's unique physiological features to verify their identity and grant access to the device or specific applications . This includes the use of firewalls to filter traffic, intrusion detection and prevention systems (IDPS) to monitor and respond to suspicious activities, virtual private networks (VPNs) for secure remote access, network segmentation to restrict access to sensitive information, and encryption to secure data in transit. The third level, application and data security, focuses on safeguarding the applications and the data they handle. This involves implementing multi-factor authentication (MFA) and role-based access control (RBAC) to ensure only authorized users have access, adopting secure coding practices to prevent vulnerabilities, encrypting sensitive data at rest, regularly updating and patching systems to protect against known vulnerabilities, and deploying

III. PROPOSED WORK

All business, government organizations and other organizations are investing a lot of money and computer memory for the security of information. Online password guessing have been known since the early days of the Internet, there is little academic on prevention techniques. This project proposes 3 levels of security. During password creation, there is an image user will select three click points or pixel positions within that image. After considering the pixel positions user must re-login and authenticate for the next level of login process i.e., OTP generation sent to the phone number.

Therefore this works encouraging users to select Image and difficult Click points to guess. Brute force and dictionary attacks on password - only remote login are now widespread and ever increasing. While preventing such attacks, enabling convenient login for legitimate users is a difficult problem. Automated Turing Tests continue to be an effective, easy to deploy approach to identify automated malicious login attempts with reasonable cost to users .The proposed work for a "Triple Guard Three-Level Security System" involves designing and implementing a comprehensive security framework with multiple layers of protection to safeguard digital assets and mitigate cybersecurity threats effectively. Here's an outline of the proposed work:

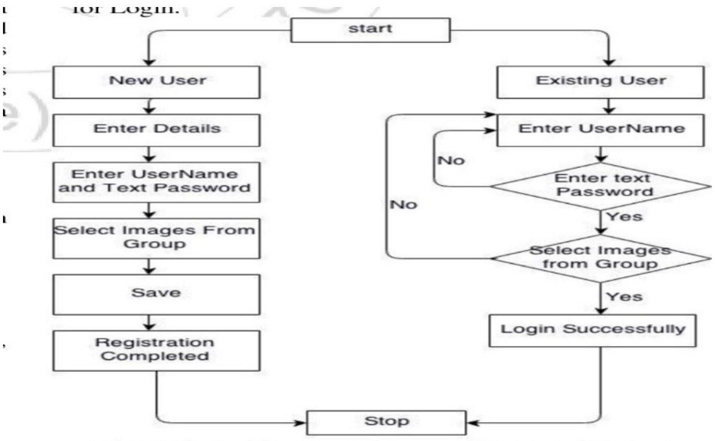


Figure 1: Architecture Diagram of Proposed System

fig 4. Illustrates architecture of proposed system

1. Layered Security Architecture Design (Guard):: The first step involves designing a layered security architecture comprising three distinct levels of defense, each providing unique security controls and mechanisms. These layers could include network security, system security, and application security, with each layer serving as a barrier to potential threats.
2. System Hardening and Access Controls (Guard 2): The second layer involves system hardening measures and access controls to protect individual devices and resources within the network. This includes strategies such as regular software patching and updates, endpoint protection (antivirus/antimalware), strong authentication mechanisms (e.g., multi-factor authentication), and role-based access controls (RBAC) to limit user privileges based on their roles and responsibilities.
3. Application Security and Data Protection (Guard 3): The innermost layer focuses on securing applications and sensitive data assets against cyber threats. This involves implementing secure coding practices, application firewalls, encryption techniques (both in transit and at rest), data loss prevention (DLP) solutions, and regular security assessments and audits to identify and remediate vulnerabilities in applications and data storage systems.
4. Continuous Monitoring and Threat Intelligence: The proposed work includes implementing continuous monitoring tools and threat intelligence feeds to proactively detect and respond to security incidents in real-time. This involves monitoring network traffic, system logs, and user activities for suspicious behavior patterns and indicators of compromise (IoCs), and leveraging threat intelligence sources to stay updated on emerging cyber threats and attack vectors.
5. Training and Awareness: Finally, the proposed work includes providing regular cybersecurity training and awareness programs to educate employees and stakeholders about security best practices, common threats, and their roles and responsibilities in maintaining the security posture of the organization. Data protection measures, including encryption and secure transmission protocols, are evaluated to safeguard sensitive information. This comprehensive approach ensures robust security, shielding the system from unauthorized access, resource misuse, and data breaches effectively. The "Triple Guard Three-Level Security System" is a comprehensive web application designed to provide robust security measures across three levels. It integrates authentication, authorization, and encryption to ensure secure access and protect sensitive data. This system incorporates advanced intrusion detection and prevention mechanisms, continuous monitoring

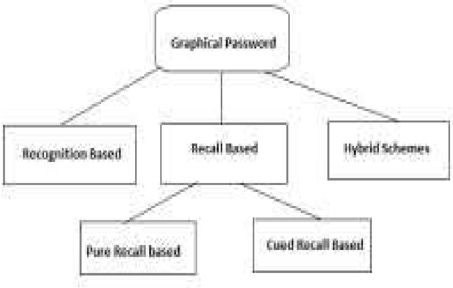


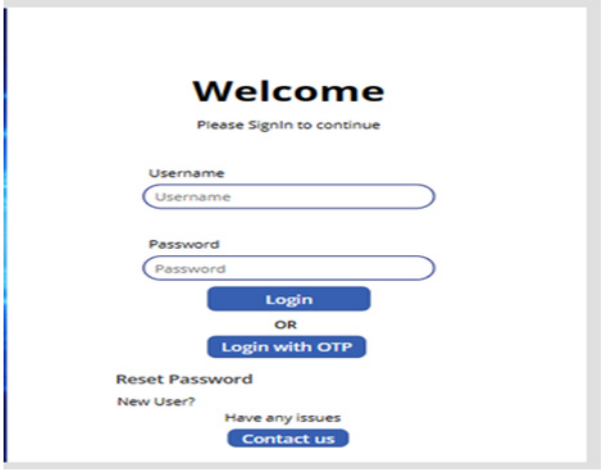
Fig 5. graphical way of representation

Waterfall Model: A sequential model developing from one phase to another without going back to handle changes.

In evaluating a user system within a triple guard, three-level security framework, the focus lies on three key aspects: user authentication, access control, and data protection.Authentication methods are scrutinized to ensure only authorized individuals gain entry. Access controls are assessed for their precision in allocating resources based on user roles.Data protection measures, including encryption and secure transmission protocols, are evaluated to safeguard sensitive information.This comprehensive approach ensures robust security, shielding the system from unauthorized access, resource misuse, and data breaches effectively.The "Triple Guard Three-Level Security System" is a comprehensive web application designed to provide robust security measures across three levels. It integrates authentication, authorization, and encryption to ensure secure access and protect sensitive data. This system incorporates advanced intrusion detection and prevention mechanisms, continuous monitoring, and adherence to secure development practices. It empowers users with knowledge through educational initiatives on security best practices. This application offers a multi-layered approach to safeguard against various threats and vulnerabilities, ensuring a secure digital environment.

IV. RESULT ANALYSIS

Complex Password Requirements: The first guard could be the complexity of the password itself. Users might be required to create passwords that meet certain criteria, such as a minimum length, a mix of uppercase and lowercase letters, numbers, and special characters. This helps ensure that passwords are not easily guessable or susceptible to brute-force attacks. It mandates the creation of complex passwords, requiring a combination of uppercase and lowercase letters, numbers, and special characters to resist brute-force attacks. That way there would be negligible chances of the bot or anyone else cracking the passwords, even if they crack the first or second level it would be impossible to crack the third. It emphasizes the need for multi-layered protection to safeguard sensitive information and prevent Unauthorized security . Triple Guard's ability to safeguard critical data assets against internal and external threats. Creating a graphical security system for authentication can enhance the user experience and security of a login system.Triple Guard encrypts data both at rest and in transit, preserving its confidentiality and integrity. Granular access controls, data masking techniques, and data loss prevention (DLP) measures further enhance Triple Guard's ability to safeguard critical data assets against internal and external threats. Authentication and security are two terms which are interrelated. Authentication is the act of confirming the exactness of an attribute of a distinct piece of data (datum) or entity.for any type of applications, sites, etc. In this system, users can first register in the system and after the registration process; the users can login to It is actually the process of confirming the identity. It is an application that is generally intended for providing security the system using the same details they provided during the registration.As this system has 3 levels of security, any intruder will not be able to hack the details of the users. The key distinction between security and responsibility is that security should take under consideration the actions of individuals making an attempt to cause destruction.



Welcome

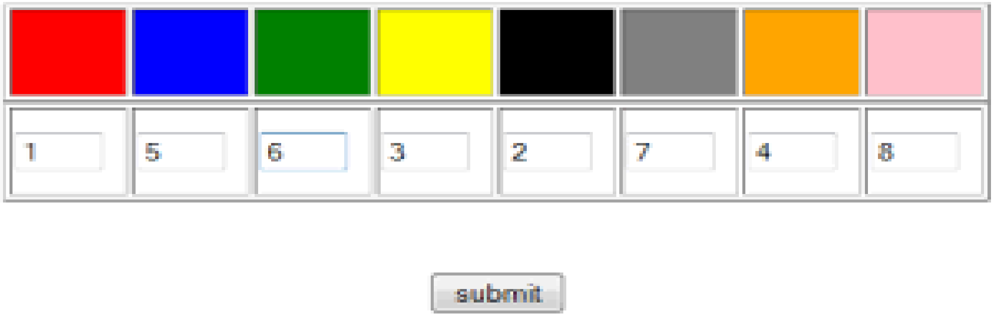
Please SignIn to continue

Username: Username

Password: Password

Fig 6 : screenshot of login credentials of user

This secondary layer enhances security by mitigating risks associated with password theft or compromise. Lastly, the system employs robust encryption techniques, hashing passwords with salted values to protect stored credentials. Even in the event of a data breach, passwords remain securely encrypted, thwarting attempts at unauthorized access. Together, these three guards fortify the login process, ensuring stringent protection against unauthorized entry. It incorporates two-factor authentication, necessitating an additional form of verification beyond the password, such as a temporary code sent to a user's mobile device. Graphic passwords are an alternative authentication method that uses images, patterns, or symbols instead of traditional alphanumeric passwords. Rather than typing in a sequence of characters, users interact with graphical elements to authenticate themselves. Role-based access control (RBAC) ensures users have appropriate resource access. Inconsistencies in access permissions were identified.**Passpoints:** Users select specific points or areas on an image as their password. When logging in, they must replicate the sequence of points they originally chose.Draw-based: Users draw a pattern or gesture on a grid or canvas. This pattern serves as their password, and they must redraw it to authenticate themselves.Innovative approaches to password protection are continually evolving, and one such method involves allowing users to upload their images as part of the authentication process. This personalized approach begins with users selecting an image of their choice during account setup, whether it be a cherished photograph, a favorite piece of artwork, or any memorable visual. A three-level security-based system involves implementing comprehensive protective measures at different layers to ensure robust defense against various threats. The first level, physical security, focuses on preventing unauthorized physical access to facilities and hardware through measures such as secure access control systems (like key card entry and biometric scanners), surveillance cameras, security personnel, and environmental controls including fire suppression systems and climate control. The second level, network security, aims to protect the network infrastructure from cyber threats and unauthorized access. This involves implementing multi-factor authentication (MFA) and role-based access control (RBAC) to ensure only authorized users have access, adopting secure coding practices to prevent vulnerabilities, encrypting sensitive data at rest, regularly updating and patching systems to protect against known vulnerabilities, and deploying Security Information and Event Management (SIEM) systems to collect and analyze security data for timely detection and response to incidents. By layering these security measures, the system ensures that if one layer is compromised, the additional layers continue to provide protection, creating a robust overall security posture.



1	5	6	3	2	7	4	8

fig 7. screenshot of password generated in graphical reprentation

Subsequently, during login attempts, users interact with their chosen image by selecting specific points, tracing patterns, or clicking on predefined areas overlaid on the image. This interaction serves as their password, with the system validating their actions against stored authentication data. To bolster security, additional factors like traditional passwords or one-time codes can complement the image-based authentication process. All uploaded images and associated data are securely encrypted and stored, ensuring protection against unauthorized access. Click-based. Similar to passpoints, users click on specific areas or objects within an image to create a sequence. They must reproduce this sequence during login. While this approach adds a personalized touch to password protection and may enhance user engagement, stringent security measures must accompany its implementation to safeguard user data and privacy.Standardization: Unlike text-based passwords, there is less standardization in the design and implementation of graphic password systems, which can lead to inconsistency and confusion for users. This interaction serves as their password, with the system validating their actions against stored authentication data. To bolster security, additional factors like traditional passwords or one-time codes can complement the image-based authentication process. All uploaded images and associated data are securely encrypted and stored, ensuring protection against unauthorized access. Click-based. Subsequently, during login attempts, users interact with their chosen image by selecting specific points, tracing patterns, or clicking on predefined areas overlaid on the image. This interaction serves as their password, with the system validating their actions against stored authentication data.

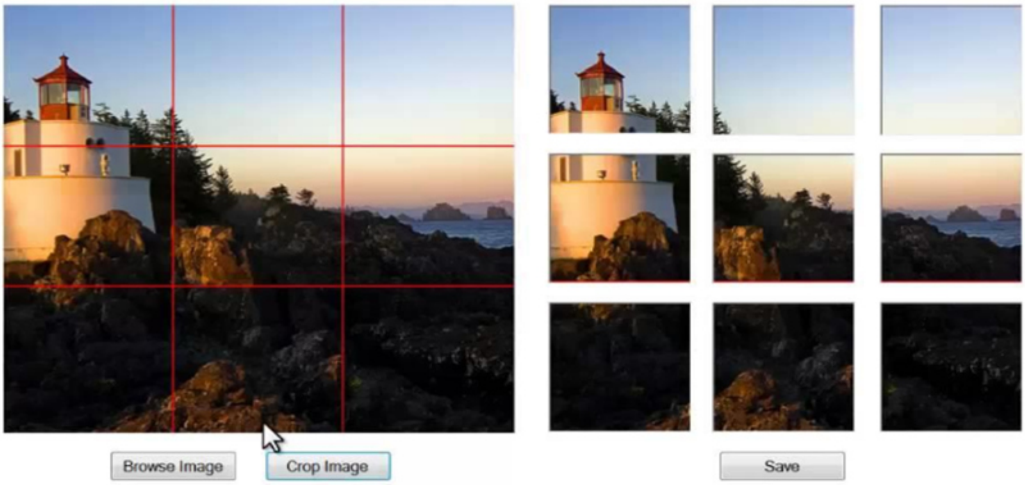


Fig 8: screenshot of the image representation of password .

Memorability : Some users find graphical patterns or images easier to remember than alphanumeric strings, potentially reducing the likelihood of forgotten passwords. Recognition-based: Users identify or recognize specific images or symbols from a set of options. This method relies on the user's ability to recall and correctly identify the predetermined images.This personalized approach begins with users selecting an image of their choice during account setup, whether it be a cherished photograph, a favorite piece of artwork, or any memorable visual. Subsequently, during login attempts, users interact with their chosen image by selecting specific points, tracing patterns, or clicking on predefined areas overlaid on the image. This interaction serves as their password, with the system validating their actions against stored authentication data. All uploaded images and associated data are securely encrypted and stored, ensuring protection against unauthorized access.

V. CONCLUSION

A three-level password security system offers a robust approach to safeguarding sensitive information and systems. This system comprises three tiers of authentication, each adding layers of defense against unauthorized access. At the first level, users provide basic credentials such as a username and password. This initial authentication step ensures that only authorized individuals can attempt to access the system.The second level introduces additional authentication factors, such as biometric data or a security token. This added layer enhances security by requiring something the user possesses or is, further reducing the risk of unauthorized access even if the initial credentials are compromised.The third level incorporates advanced security measures like multi-factor authentication or adaptive authentication. These adaptive methods dynamically adjust the level of authentication based on contextual factors, such as location or behavior patterns, adding an extra dimension of protection against sophisticated threats. In conclusion, a three-level password security system provides comprehensive protection by combining multiple authentication factors and adaptive measures. By implementing this approach, organizations can significantly reduce the risk of unauthorized access and enhance overall cybersecurity posture. It provides a robust defense against cyber threats by implementing multiple layers of protection. It starts with perimeter defense, followed by system hardening and access controls, and concludes with application security and data protection. Integration, continuous monitoring, and training ensure a comprehensive and resilient security posture. This approach mitigates risks effectively and maintains the confidentiality, integrity, and availability of digital assets in today's cybersecurity landscape. This system incorporates advanced intrusion detection and prevention mechanisms, continuous monitoring, and adherence to secure development practices. It empowers users with knowledge through educational initiatives on security best practices. This application offers a multi-layered approach to safeguard against various threats and vulnerabilities, ensuring a secure digital environment.

VI. FUTURE SCOPE

The scope and enhancement of a "Triple Guard" approach in software development involve expanding its coverage, effectiveness, and adaptability to address evolving threats and requirements. Here's how you can define the scope and enhance the "Triple Guard" strategy: Expanding Guard Layers: Consider adding more layers beyond the initial three guards to address specific risks or vulnerabilities unique to your application domain. For example, you might introduce a data encryption guard to protect sensitive information at rest or in transition. Continuous Improvement: Establish a culture of continuous improvement by regularly evaluating the performance and efficiancy of guard mechanisms. Collect feedback from incident reports, security audits, and penetration on tests to identify areas for enhancement and refinement. The future scope of employee ID card generator in Django is very promising. Django is a powerful web framework that makes it easy to develop and deploy web applications. With Django, you can quickly and easily create an employee ID card generator that meets the needs of your organization.

Here are some specific examples of how employee ID card generators could be used in the future: Employee ID card generators could be used to improve security by making it more difficult for unauthorized individuals to access secure areas. Employee ID card generators could be used to improve efficiency by automating tasks such as timekeeping and access control. Employee ID card generators could be used to improve communication by providing employees with a way to quickly and easily identify themselves. Employee ID card generators could be used to improve compliance by providing a way to track employee attendance and hours worked. Overall, employee ID card generators have the potential to improve the efficiency, security, and communication of businesses. As the technology continues to develop, we can expect to see even more innovative and beneficial uses for employee ID card generators in the future. The security mechanism of the system may be improved to protect the privacy of the users. Further research may be conducted in terms of feedback on the developed system. Finally, future research may be conducted to make use of the results of this study for a deeper analysis of issues and concerns involving the maintainability and sustainability of the system.

VII. REFERENCES

[1] Usha Kosarkar, Gopal Sakarkar, Shilpa Gedam (2022), "An Analytical Perspective on Various Deep Learning Techniques for Deepfake Detection", 1st International Conference on Artificial Intelligence and Big Data Analytics (ICAIBDA), 10th &amp; 11th June 2022, 2456-3463, Volume 7, PP. 25-30, https://doi.org/10.46335/IJIES.2022.7.8.5

[2] Usha Kosarkar, Gopal Sakarkar, Shilpa Gedam (2022), "Revealing and Classification of Deepfakes Videos Images using a Customize Convolution Neural Network Model", International Conference on Machine Learning and Data Engineering (ICMLDE), 7th &amp; 8th September 2022,26362652, Volume 218
PP. 2636-2652, https://doi.org/10.1016/j.procs.2023.01.237

[3] Usha Kosarkar, Gopal Sakarkar (2023), "Unmasking Deep Fakes: Advancements, Challenges, and Ethical Considerations", 4th International Conference on Electrical and Electronics Engineering (ICEEE),19th &amp; 20th August 2023, 978-981-99-8661-3, Volume 1115, PP. 249-262, https://doi.org/10.1007/978-981-99-8661-3_19

[4] Usha Kosarkar, Gopal Sakarkar, Shilpa Gedam (2021), "Deepfakes, a threat to society", International Journal of Scientific Research in Science and Technology (IJSRST), 13th October 2021, 2395-602X, Volume 9, Issue 6, PP. 1132-1140, https://ijsrst.com/IJSRST219682

[5] Usha Kosarkar, Gopal Sakarkar (2024), "Design an efficient VARMA LSTM GRU model for identification of deep-fake images via dynamic window-based spatio-temporal analysis", International Journal of Multimedia Tools and Applications, 8 th May 2024, https://doi.org/10.1007/s11042-024-19220-w

[6] https://www.researchgate.net/publication/321698441_Graphical_Password_Authentication_using_Images_Sequence

[7] Security Analysis and Implementation of JUIT-IBA System using Kerberos Protocol, Proceedings of the 7th IEEE International Conference on Computer and Information Science, Oregon, USA, pp. 575-580, 2008. http://www.ijedr.org

_[8] Chris Ullman and Lucinda Dykes, Beginning Ajax (Programmer to Programmer), Paperback, March 19, 2007. www.ijesr.org