Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Advancing Authentication Systems with Multi-Level Approaches

Reddyvari Venkateswara Reddy, Sambari Manoj, Marri Samhitha Reddy, Samantha Juan
Associate Professor, Department of CSE (Cyber Security), CMR College of Engineering and Technology, Hyderabad, India
Student, Department of CSE (Cyber Security), CMR College of Engineering and Technology, Hyderabad, India

***Abstract*— Multi-Level authentication systems have become a cornerstone in safeguarding sensitive information from unauthorized access. At the foundational level, the system employs traditional username-password authentication, a widely adopted method for initial access control. Users provide a unique combination of credentials during registration, which are securely stored and verified uponsubsequent logins. In the second level introduces an innovative image-based authentication mechanism. During registration, users select an image that serves as their personal authentication marker. Upon login, users must re- upload the same image, verifying their identity through visual recognition, adding multiple layers of security against password breaches or brute force attacks. The third and finallevel employs cutting-edge technology by integrating Convolutional Neural Networks (CNNs) to generate handwritten CAPTCHAs (Completely Automated PublicTuring test to tell Computers and Humans Apart). CAPTCHAs challenge users to prove their human identity bydeciphering distorted text or images.**

***Keywords:* Multi-level authentication, security, username and password authentication, image upload, graphical password, captcha, CNN algorithm, MERN stack, Flask, authentication factors.**

I. INTRODUCTION

In an era marked by using rapid technological development and the pervasive presence of digital structures, making sure the safety of sensitive statistics and digital belongings has grown to be a paramount problem. traditional strategies of authentication, consisting of relying totally on usernames and passwords,have proven to be inadequate in the face of more and more state-of-the-art cyber threats. As hackers employ ever-evolving processes to breach security features, businesses and individuals alike are in search of more sturdy answersto defend their records.

Multi-level authentication (MLA), a dynamic method to authentication that is going beyond the confines of traditional techniques. At its center, MLA calls for customers to offer a couple of authentication factors, thereby adding layers of protection to the authentication procedure. By incorporating diverse authentication elements, such as a factor the user knows (e.g., a password), something the user has (e.g., a token or smartphone), and something the user is (e.g., biometric data), MLA significantly bolsters the security of digital systems.

MLA is rooted in the precept of protection in depth, which advocates for the deployment of a couple of layers of safety controls to defend towards various assault vectors.with the aid of requiring attackers to bypass multiple authentication barriers, MLA makes it exponentially more difficult for people to have the advantage of gettingright of entry by unacceptable means, to touchy facts or structures. This method however now is not most effective but strengthens protection and additionally gives a more reliable method of verifying the identification of users.

Within the context of this venture, we are trying to find to harness the strength of MLA to develop an software that exemplifies the concepts of sturdy authentication. by using integrating three distinct tiers of authentication, every with its own precise challenges and verification techniques, our objective is to make a comprehensive safety framework that guards against a extensive range ofpotential threats. through the implementation of this MLAapplication, we endeavour to raise the requirements of protection in digital environments and offer users with the peace of thoughts they deserve in an increasing number ofinterconnected world.

II. LITERATURE REVIEW

1. Anil K. Jain, Arun Ross, Karthik Nandakumar. "Biometric Authentication: A Review." IEEE Transactions on Pattern Analysis and Machine Intelligence, 2004.

Biometric Authentication: A Review, provides a comprehensive review of biometric authentication methods, discussing various biometric modalitiessuch as fingerprint, face, iris, and voice recognition. It examines the challenges, advantages, and limitations of biometric authentication systems, transforming it into a valuable resource for learningthe state-of-the-art in biometrics.

2. Jiliang Zhang, Xiao Tan, Xiangqi Wang, Aibin Yan, Zheng Qin. "T2FA: Transparent Two- Factor Authentication" 15 June 2018. Transparent two-factor authentication (T2FA), a singular technique to transparent two-element authentication. T2FA pursuits to decorate safety while minimizing person disruption via seamlessly integrating the second authentication issue into theconsumer's everyday engagement with the machine. The paper provides the design, implementation, andevaluation of T2FA, highlighting its effectiveness and value.

3. Jaesik Lee, Youngseok Oh. "A Study on Providing the Reliable and Secure SMS Authentication Service" in conf. Intl Conf on Ubiquitous Intelligence and Computing, 9-12 Dec2014.
   This conference paper investigates the reliability and security of SMS-based authentication services. It examines the vulnerabilities associated with SMS authentication, such as SIM swapping attacks, and proposes strategies to mitigate these risks. The paper presents a discussion on the effectiveness of SMS authentication in ensuring both reliability and security for users.

4. Northcutt, S., Novak, J. I., & winters, S. (2002). Network Intrusion Detection: An Analyst's Handbook. New Riders.
   It contributes to the literature with a focal point on intrusion detection, a complementary issue to firewalls. The paper emphasizes the synergy among intrusion detection and community-level firewalls in fortifying networks towards state-of-the-art attacks.

5. Scott Ruoti, Jeff Andersen, Kent Seamons. "Strengthening Password based Authentication" , 2016.
   This explores techniques for strengthening password-based totally authentication structures. It discusses various techniques, which include password hashing, salting, and multi-issue authentication, to improve the safety of password- based authentication. The paper offers experimental results and sensible tips for enhancing the resilience of password-based totally systems in opposition to commonplace assaults.

6. Himika Parmar, Nancy Nainan, Sumaiya Thaseen. "Generation of Secure One-Time Password Based on Image Authentication", October 2012.
   This conference proposes a way for producing at ease one-time passwords based totally on photograph authentication. It offers an set of rules for encoding textual passwords into photos, which can then be used as one-time passwords for authentication purposes. The discussion focuses on blessings and limitations of photo-primarily based authentication and evaluates the safety residences ofthe proposed technique.

III. OBJECTIVE

The goal of this documentation is to offer a comprehensive and specified assessment of a multi- stage authentication (MLA) undertaking designed to beautify security features for person authentication in virtual structures. With cyber threats turning into more and more sophisticated, traditional techniques of authentication, along with depending completely on usernames and passwords, are no longer enough to shield sensitive data and systems. As such, this mission aims to deal with this undertaking by way of imposing MLA, which involves requiring customers to offer multiple authentication elements.

The number one attention of the MLA mission is to integrate 3 awesome tiers of authentication, every serving as a further layer of safety past conventional username and password combos. via incorporating numerous authentication strategies at each degree, which includes photo add/graphical password and captcha the application of CNN, the project seeks to improve the authentication procedure enable it to be more resilient to capacity intrusions.

This documentation will delve into the rationale at the back of adopting MLA as a security measure and provide special descriptions of each authentication stage, consisting of the underlying methodologies and technology employed. moreover, it'll include a thorough literature overview, referencing relevant studies papers and research inside the field of legitimacy and security.

Moreover, the documentation will outline the blessings of enforcing MLA, together with superior protection, decreased risk of unauthorized get right of entry to, and progressed safety of touchy facts. it will additionally gift the consequences of initial checking out performed on the MLA utility, demonstrating its effectiveness in thwarting potential cyber-assaults.

IV. SYSTEM REQUIREMENTS

1. Hardware: Multi-core processors (e.g., Intel Xeon, AMD Ryzen) for handling concurrent requests efficiently. Sufficient RAM (8GB) to accommodate the expected workload and memory requirements of the applications and databases
2. Operating System: Windows is the operating system that is used for web server environment due to stability, security, and cost-effectiveness.
3. Robust Backend Infrastructure: The backend infrastructure serves as the core of the authentication system, responsible for processing user authentication requests, managing user accounts, and ensuring the security and honesty ofauthentication processes.
4. CNN Model for Captcha Generation and Verification: Convolutional Neural Network (CNN) models are employed for generating and verifying Captchas, providing another layer of security against automated attacks and ensuring human verification.
5. Safe Database to hold Authentication records: The safe database stores authentication data, including user credentials, authentication logs, and session information, ensuring data integrity and confidentiality.

Tools and Technologies Required for Multi-level Authentication Implementation:

1. MongoDB: Classified as a NoSQL database, MongoDB uses BSON (Binary JSON) to store datain a versatile JSON-like format. Thanks to its schema-less architecture, it allows different types of data to be stored within a unified collection.

2. Express.js: It is a minimum and flexible Node.js internet application framework that provides a robust set of functions to expand internet and mobile packages. It allows the development of server-facet applications in JavaScript

3. React: Facebook developed the React JavaScript library for UI design. Making interactive and dynamic user interfaces simple, it enables developers to design reusable UI components that maintain their state.

4. Node.js: Built on top of Chrome's V8 JavaScript engine, Node.js is a JavaScript runtime. It is perfect for creating server-side apps since it allows developers to run JavaScript code outside of a web browser. It is lightweight and efficient because Node.js offers an event-driven, non-blocking I/O architecture.

5. Python: High-level programming languages like Python are renowned for being straightforward, readable, and flexible. Among the most widely used programming languages in the world today is Python. Libraries like TensorFlow or PyTorch are available in Python's vast ecosystems to help construct and train Convolutional Neural Networks (CNNs) that can effectively recognize handwrittenletters.

6. Flask: Flask is a lightweight and flexible micro-framework and it simplifies the building of RESTful APIs for captcha generation and verification. Flask's integration capabilities make it easy to incorporate the trained CNN model into the authentication process, enabling users to generate and verify handwritten captchas securely. This combination ensures robust security measures while providing a user-friendly authentication experience for the system's third level.

V. PROBLEM DEFINITION

The principle challenge addressed by means of this undertaking is the inherent vulnerability of single-component authentication systems to protection breaches. commonplace security threats, such as password robbery, brute-force assaults, and phishing attempts, pose widespread risks to person debts and touchy information. To mitigate these dangers, Multi- level Authentication (MLA) introduces extra layers ofprotection, making it extra difficult for attackers to compromise user accounts or take advantage and gain unauthorized right of entry to blanketed structures. via enforcing MLA with three wonderful authentication degrees, we aim to enhance safety and offer customerswith a much better authentication to enjoy.

VI. EXISTING SOLUTIONS

Google's Two-Factor Authentication (2FA): Google presents a two-factor authentication system that mixes something the user is aware of (password) with something the consumer has (a mobile device). Users obtain a one-time code on their cellular gadgets, including a further layer of safety to their Google accounts.

1. Microsoft Azure Multi-Factor Authentication: Microsoft Azure offers a secure Multi-component Authentication as a part of its identification and get right of entry to control solutions. It also supports diverse authentication methods, such as cell app verification, cellphone call verification, and text message verification.

2. Duo Security:
Duo security is a famous multi-element authentication provider that provides a number of authentication methods, such as push notifications, one-time passcodes, and biometrics. It integrates with numerous structures and packages to offer a further layer of safety.

VII. LIMITATIONS OF THE EXISTINGSYSTEM

1. Dependency on Mobile Device: Google's 2FA relies heavily on the person's mobile tool for receiving one-time codes. This dependency can be aproblem if the user loses access to their cellular device or encounters problems with it.
2. Complexity for End Users: Enforcing Multi-issue Authentication with Microsoft Azure may also introduce complexity for quit customers, mainly those less acquainted with the authentication methods supported.
3. Cost: While as Duo security offers sturdy multi- issue authentication talents, it can include related fees for organizations, mainly for massive user bases or extra functions past basic authentication.
4. User Experience: Whilst Duo protection gives quite a number authentication strategies, the consumer revel in might also range relying on the selected approach, and some customers can also find positive authentication techniques much less intuitive or convenient.

VIII. WORK FLOW

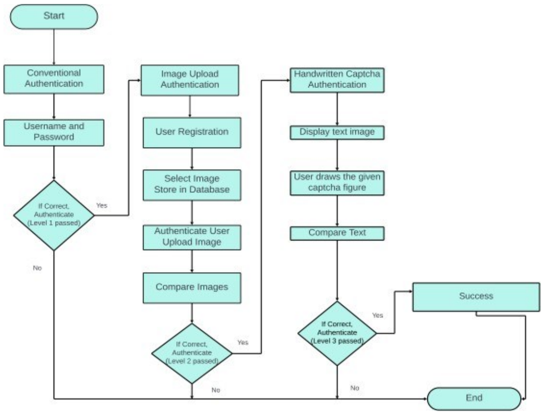

Start
Conventional Authentication
Username and Password
If Correct, Authenticate (Level 1 passed)
Yes
No
Image Upload Authentication
User Registration
Select Image Store in Database
Authenticate User Upload Image
Compare Images
If Correct, Authenticate (Level 2 passed)
Yes
No
Handwritten Captcha Authentication
Display text image
User draws the given captcha figure
Compare Text
If Correct, Authenticate (Level 3 passed)
Yes
No
Success
End

Fig-1: Work Flow

1. User Registration: Customers register with the application with the aid of providing a username and password.
2. Level 1 Authentication (Username and Password): Upon login, users undergo the first level of authentication the usage of their registered username and password.
3. Level 2 Authentication (Graphical password): If the Level 1 authentication is successful, users proceed to the second level,where they select an image or create a graphical password using the MERN stack.
4. Level 3 Authentication (Captcha Using CNN): After successful level 2 authentication, customers encounter the third level, where they engage with a captcha generated via a CNN set of laws implemented the usage of Flask. This captcha may contain typing text or drawing a number, that is then confirmed through the CNN set of rules.
5. Access Granted: If customers bypass all three tiers of authentication successfully, they gain get entry to the application's covered sources.
6. Access Denied: If customers fail to authenticate at any stage, get admission to the application's assets is denied, and appropriate error messages are displayed.
7. Logging and tracking: gadget logs and monitors music authentication attempts and any suspicious activities for security analysis and audit purposes.

IX. ARCHITECTURE

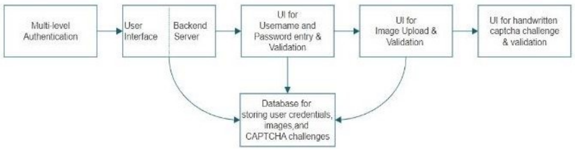

Multi-level Authentication
User Interface
Backend Server
UI for Username and Password entry & Validation
UI for Image Upload & Validation
UI for handwritten captcha challenge & validation
Database for storing user credentials, images,and CAPTCHA challenges

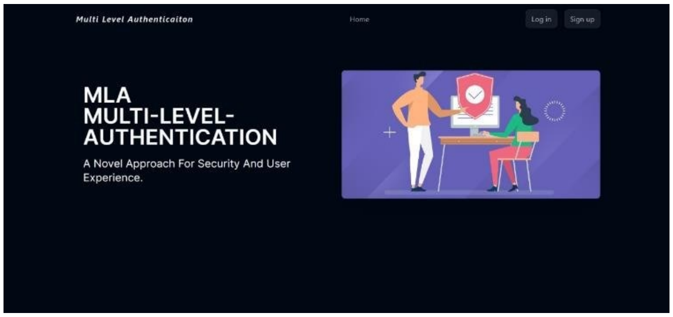
Fig-2: Architecture

1. User Interface (UI) for username & password entry: Users input their credentials, which are validated against specified criteria. Validated data is sent to the backend server.
2. UI for image upload & validation: Users upload an image, verified by format and size, then forwarded to the backend for comparison with stored data.
3. UI for handwritten CAPTCHA challenge: Users respond to CAPTCHA challenges, ensuring accuracy, and their responses are sent to the backend for validation.
4. Backend Server: Handles authentication logic, verifying credentials, comparing images, and validating CAPTCHA responses, interacting with thedatabase.
5. Database for storing user data: Stores user credentials, uploaded images, and CAPTCHA challenges, ensuring data integrity and confidentiality. The server retrieves necessary information during authentication

X. CONCLUSION

The proposed multi-degree authentication machine introduces a comprehensive and innovative approach to enhance safety at the same time as making sure user- friendly authentication. The machine includes 3 layers, every designed to give a completely unique and powerful way of verifying person identification. The multi-layered method is going past traditional methods, making sure a strong defense in opposition to unauthorized get right of entry to. It combines user-pleasant elements, including photograph upload authentication, with advanced security measures like captcha the use of CNN authentication. The system is adaptable to various consumer eventualities, supplying a stability among protection and usability.

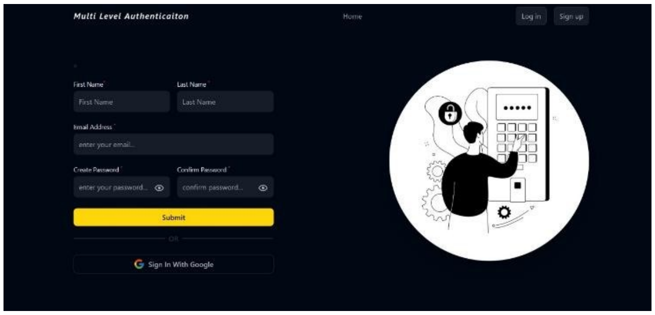
XI. RESULTS



MLA
MULTI-LEVEL-AUTHENTICATION

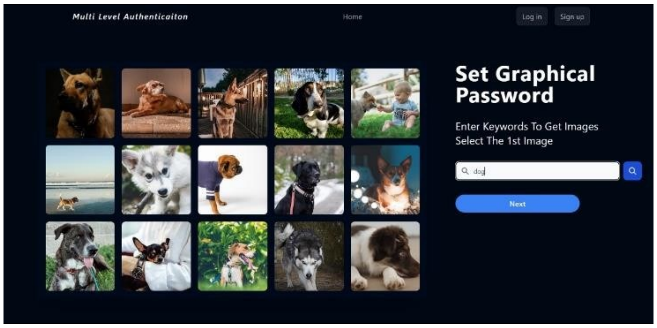
A Novel Approach For Security And User Experience.

Fig-3: Homepage



First Name*: First Name
Last Name*: Last Name
Email Address*: enter your email...
Create Password*: enter your password...
Confirm Password*: confirm password...

Fig-4: Sign-up form

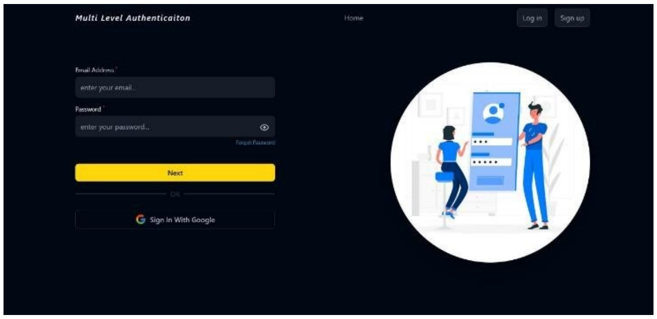


Set Graphical Password

Enter Keywords To Get Images
Select The 1st Image

dog

Fig-5: Setting graphical password after sign up



Email Address*: enter your email...
Password*: enter your password...

Fig-6: Login form

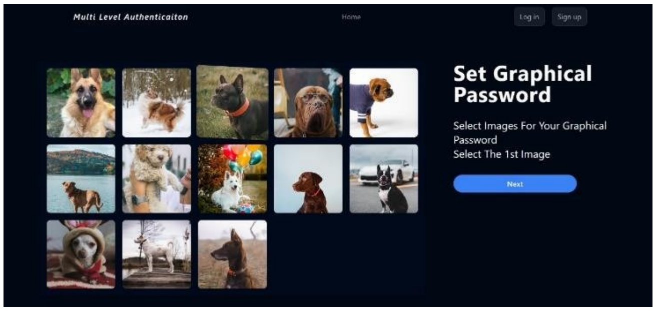

Multi Level Authenticaiton
Home
Log in
Sign up
Set Graphical Password
Select Images For Your Graphical Password
Select The 1st Image
Next

Fig-7: Selecting graphical password after login

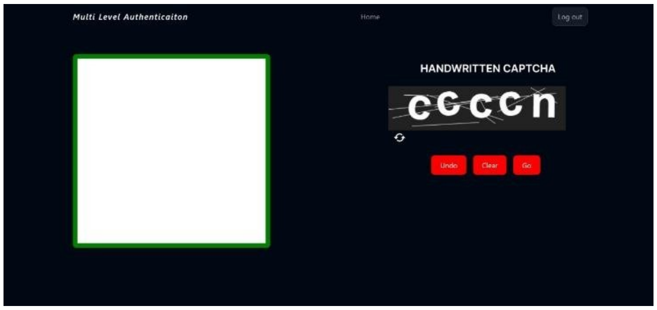


Fig-8: Handwritten Captcha

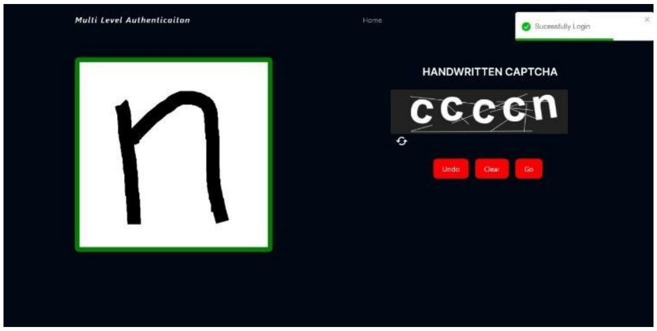

Sucessfully Login

Fig-9: Login success

XII. REFERENCES

1. Anil K. Jain, Arun Ross, Karthik Nandakumar “Biometric Authentication: A Review.” IEEE Transactions on Pattern Analysis and Machine Intelligence, 2004.
2. Jiliang Zhang, Xiao Tan, Xiangqi Wang, Aibin Yan, Zheng Qin “T2FA: Transparent Two-FactorAuthentication” in conf. IEEE, 15 June 2018.
3. Jaesik Lee, Youngseok Oh “A Study on Providing the Reliable and Secure SMS Authentication Service” in conf. Intl Conf on Ubiquitous Intelligence and Computing, IEEE, 9-12 Dec 2014, Bali, Indonesia.
4. Scott Ruoti, Jeff Andersen, Kent Seamons“Strengthening Password-based Authentication”in conf. Twelfth Symposium on Usable Privacy and Security, United States,2016.
5. Himika Parmar, Nancy Nainan, Sumaiya Thaseen “Generation of Secure One-Time Password Based on Image Authentication” in conf. The Fourth International Workshop onComputer Networks & Communications,October 2012.
6. F. Deivendran, M. Arulmozhivarman, V. Sankara Subramanian "Multilevel Authentication: A Survey" in International Journal of ComputerApplications, Vol. 168, No. 7, 2017.
7. Ajay Kumar, Santosh Kumar "A Review Paper on Multilevel Authentication Techniques for Secure Data Access in Cloud Computing" in International Journal of Computer Science and Mobile Computing, Vol. 5, No. 4, 2016.
8. V. Shanthi, T. Bhuvaneswari "A Study on Multilevel Authentication Techniques in Wireless Sensor Networks" in International Journal of Advanced Research in Computer Science, Vol. 8, No. 3, 2017.
9. Anamika Jain, Amit Kumar Jain "Multilevel Authentication Mechanism in Cloud Computing" in the International Journal of Computer Applications, Vol. 162, No. 9, 2017.
10. R. Rajesh, S. Padmavathi "Multilevel Authentication System Using Biometric and Graphical Password" in International Journal of Engineering and Technology, Vol. 5, No. 3, 2013.