[1] **Natasha Mhaskar**
[2] **Dr. Dhananjay Dakhane**
[3] **Vaibhav Narawade**

User Authenticate Using Multifactor Authentication

Journal of Electrical Systems

Abstract: - This study delves into sophisticated multi-faceted approaches. authentication techniques to enhance system security. As cyber-attacks become increasingly sophisticated, it is crucial to continuously update our systems to protect them from malicious hackers. Our study identifies that hackers often deploy multiple systems to infiltrate or compromise a target. They may obscure or alter system details, dynamically change IP addresses, or switch networks during an attack. In response, we have developed a website that captures the device ID upon any interaction. When a user tries to log in, they must provide their username and password. If these credentials are verified, the system then generates a file containing the username, device ID, and the first three digits of the password, which is encrypted using a hashing algorithm and stored in the database. Successful login is contingent upon matching the file details. In the event of a device ID mismatch, the user is prompted for a live image capture. If the captured image is verified as accurate, access is granted; otherwise, access is denied. This research employs hashing algorithms to ensure secure data transfer between endpoints, providing a robust defense against unauthorized access. This approach offers enhanced security for various sectors, including banking, insurance, and healthcare, safeguarding login credentials from cyber threats.

Keywords: Multi-factor authentication, Face recognition, Authentication, Information Security.

I. INTRODUCTION

In today's digital environment, maintaining strong system security is crucial because of the increasing prevalence of cyber threats. Traditional password-based authentication methods are increasingly inadequate in safeguarding sensitive information, the widespread adoption of Multiple kinds of verification are required for users to use Multi-Factor Authentication (MFA), which considerably increases security. Getting there

substantially more difficult for unauthorized parties to breach systems [1].

Authentication methods typically fall into a few key Categories include knowledge-based techniques, biometrics, and hybrid approaches. Knowledge-based techniques, also known as single-factor authentication, rely on credentials such as usernames, passwords, PIN codes, patterns, and OTPs. While convenient, these methods are vulnerable to attacks due to their reliance on easily compromised data. Biometrics, which include fingerprint, facial recognition, voice, and iris scanning, offer improved security but can be problematic if natural incidents or changes affect the biometric data, potentially locking out legitimate users.

Multi-factor authentication (MFA) fortifies security by combining various Verification techniques include things the user knows (like a password), things the user owns (like a hardware token or smartphone), and things the user is (like biometric data). This layered strategy provides a more robust defense against unauthorized access, as attackers would need to compromise multiple security layers at once.

A significant challenge in MFA is distinguishing between legitimate user devices and potential attackers, especially as sophisticated hackers employ dynamic techniques like changing IP addresses and hiding system details to evade detection. To address these issues, advanced security measures must be continually developed and adapted to counter evolving threats.

The structure of this document is as follows: Section II reviews the body of current literature. on authentication methods. Sections III and IV present our proposed MFA architecture and its design. Section V discusses future research directions, and Section VI provides feasibility results [3]. Finally, Section VII summarizes the findings and conclusions. In summary, as cyber threats become more advanced, integrating multifactor authentication is essential for robust security and protection of digital assets.

[1] Natasha Mhaskar,Department of Computer Engineering , Ramarao Adik Institute Of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai.
[2] Dhananjay Dakhane,Department of Computer Engineering , Ramarao Adik Institute Of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai. dhananjay.dakhane@rait.ac.in
[3] Vaibhav Narawade,Department of Computer Engineering , Ramarao Adik Institute Of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai. vaibhav.narawade@rait.ac.in
* Corresponding Author Email: natasha.mhaskar@gmail.com

II. LITERATURE SERVEY

The study of this "Multifactor Authentication Schemes for Multiserver Based Wireless Application: A Review" by Y. Nogia, S. Singh, and V. Tyagi, presented at the 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), provides a comprehensive review of multifactor authentication (MFA) schemes in the context of multiserver wireless applications. The authors explore various MFA techniques employed to enhance security in environments where multiple servers are involved.

The study highlights the growing importance of MFA due to the increasing prevalence of cyber threats and the need for robust security measures. Multifactor authentication, which requires users to provide multiple forms of verification before gaining access, is essential for protecting sensitive information and ensuring secure communications. The paper categorizes and examines different MFA schemes, analyzing their effectiveness, strengths, and limitations in the context of multiserver wireless systems. The review includes an assessment of various authentication factors such as something you know (e.g., passwords), something you have (e.g., tokens or smart cards), and something you are (e.g., biometrics). By comparing and contrasting these methods, the authors provide insights into their applicability and performance in multiserver scenarios, where security challenges are more complex due to the involvement of multiple interacting servers.

Overall, the paper underscores the need for continued research and development in MFA technologies to address emerging threats and improve the reliability and efficiency of authentication processes in wireless networks. This comprehensive review serves as a valuable resource for researchers and practitioners seeking to understand and implement effective multifactor authentication solutions in modern wireless applications.

[2]. A. A. S. AlQahtani, B. Al Smadi, and H. Alamleh wrote a paper titled "Secure Mobile Payment Architecture Enabling Multi-Factor Authentication," which was presented at the Systems and Information Engineering Design Symposium (SIEDS) in Charlottesville, Virginia, USA,examines advanced architectural frameworks aimed at improving the security of mobile payment systems through the use of multi-factor authentication (MFA).This study delves into the development of a robust mobile payment architecture that integrates MFA to safeguard transactions and user

data against potential security threats. The proposed architecture aims to address the inherent vulnerabilities in mobile payment systems by incorporating multiple layers of verification. MFA, a validated security measure, integrates multiple authentication elements include things like the user's knowledge (passwords), possessions (security tokens), and identity (biometric data). To strengthen the authentication process, leverage what the user is (biometric identifiers) and has (smartphones or hardware tokens). The authors meticulously detail the design and operational aspects of their proposed architecture, highlighting its ability to deliver a high level of security while maintaining user convenience. The paper evaluates the efficacy of their approach in mitigating risks associated with mobile payments and discusses the implications for both developers and users.

Alamleh, AlQahtani, and Al Smadi's research contributes to the ongoing evolution of mobile payment security by presenting a novel framework that leverages MFA to enhance transaction integrity and user trust. Their work underscores the critical importance of adopting advanced security measures in the rapidly growing domain of mobile financial services

[3] Introduces an innovative approach to enhancing security for voice-controlled devices by employing a hands-free two-factor authentication system that leverages Wi-Fi location technology. The research addresses the challenge of securing voice-activated devices, which often face vulnerabilities due to their continuous listening capabilities and the potential for unauthorized access. The proposed "Smartphone-key" system integrates two-factor authentication (2FA) with Wi-Fi location data to create a seamless yet robust security mechanism. By utilizing the unique spatial information provided by Wi-Fi networks, the system verifies the physical proximity of a user's smartphone to the voice-controlled device, thereby adding an additional layer of authentication. This hands-free solution enhances user convenience while maintaining high security standards. The system eliminates the need for manual input of authentication codes, streamlining the user experience. Additionally, the integration of Wi-Fi location data allows for context-aware authentication, improving the overall effectiveness of the security measure. The paper details the design, implementation, and evaluation of the "Smartphone-key" system, providing insights into its performance and potential applications. Alattar, Abbes, and Zerai's work contributes to advancing security protocols for voice-controlled technologies, addressing both usability and protection concerns in a rapidly evolving digital landscape.

[4]This innovative approach to multi-factor authentication (MFA) by introducing a system that consolidates the authentication process into a single finger swipe. The authors propose a novel method that integrates multiple authentication factors into a streamlined, user-friendly gesture. The system combines biometric data with

contextual information to verify user identity efficiently while minimizing user effort. The research addresses the challenge of balancing robust security with ease of use. Traditional MFA methods often require multiple steps or additional devices, which can be cumbersome and reduce user satisfaction. By leveraging a single finger swipe, the proposed solution aims to enhance user convenience without compromising the security provided by multi-factor authentication. The authors detail the technical implementation and evaluation of their system, demonstrating its reliability and effectiveness in various scenarios. The paper discusses the underlying algorithms, system architecture, and performance metrics, offering a comprehensive analysis of the proposed authentication method. Liu, Cui, Zou, Han, Lin, and Ren's this work represents a notable advancement in the field. Of user authentication, providing a practical solution that addresses both security concerns and user experience. Their approach promises to simplify the authentication process while maintaining high standards of reliability and prediction focuses on employing machine learning techniques to enhance fraud detection in banking transactions.

[5]In their study, Acharya and Shelve investigate the use of cutting-edge machine learning algorithms in financial transaction fraud detection and prevention. The paper addresses the growing concern of fraud within the banking sector and highlights how traditional methods are increasingly insufficient due to the sophisticated nature of modern fraud schemes.

The authors propose a machine learning-based approach that leverages various algorithms to examine transaction patterns, identify anomalies, and flag potentially fraudulent activities with high accuracy. By training models on historical transaction data, the system is designed to recognize unusual behaviors and patterns that may indicate fraudulent behavior. The paper provides an in-depth description of the machine learning models employed, the features analyzed, and the performance metrics assessed. Acharya and Shekel's work underscores the potential of machine learning to significantly improve the efficiency and effectiveness of fraud detection systems. Of fraud detection systems in banking. Their approach is designed to improve security while also reducing false positives and minimizing disruptions to legitimate transactions. The study contributes to the ongoing efforts to combat financial fraud using innovative technological solutions.

[6] The study introduces an advanced framework for implementing authentication systems in large, multi-site enterprises. The research focuses on the development of a robust two-factor authentication (2FA) framework combined with continuous authentication mechanisms. This integrated approach aims to enhance security across complex organizational environments by combining traditional authentication methods with ongoing verification processes. The framework is designed to address the challenges faced by large enterprises, where traditional authentication methods may fall short due to the scale and diversity of user interactions and access points.

The authors propose a solution that continuously monitors and verifies user identities, beyond the initial login phase. By employing a two-factor approach— such as something the user knows (a password) and something the user possesses (a security token) or biometric data)—the framework ensures a higher level of security. Continuous authentication further strengthens this by analyzing user behavior and contextual data to detect any anomalies or unauthorized activities in real-time. Déncs-Fazakas, Kael, and Flexner's work provides a detailed exploration of their proposed framework, including its design, implementation, and evaluation. Their approach aims to enhance security measures in large enterprises, ensuring that access remains tightly controlled and monitored throughout the user's session. The study contributes to advancing the field of enterprise security by integrating continuous and multi-factor authentication strategies.

[7]The third International Cyber Resilience Conference (CRC) featured a presentation by M.A. Hassan and Z. Shakur titled "A Secure Multi-Factor User Authentication Framework for Electronic Payment Systems". The authors address the critical need for robust security measures in electronic payment systems, where the risk of unauthorized transactions and fraud is significant. Their proposed framework integrates multiple authentication factors to provide a comprehensive security solution that goes beyond traditional single-factor methods. This multi-layered approach includes various types of authentication, such as something the user knows (e.g., passwords), something the user possesses (e.g., OTPs or hardware tokens), and something the user is (e.g., biometric identifiers). Hassan and Shakur's framework is designed to address the vulnerabilities associated with electronic payments by ensuring that access to sensitive financial transactions is tightly controlled. The paper outlines the architecture of the proposed system, detailing how the different authentication factors are combined to enhance security. Additionally, the authors discuss the implementation challenges and potential benefits of their framework, emphasizing its ability to significantly reduce the risk of fraudulent activities. Overall, their work contributes to the field of cybersecurity by offering a robust solution for securing electronic payment systems. The proposed MFA framework aims to improve user trust and protect financial transactions through advanced, multi-faceted authentication techniques.

[8]The study titled "Multi-Factor Authentication for System Login," authored by B.O. Amsalem and A. I. an lshoshan, in their research, AL Salem and Al Shoshana explore the integration of MFA into system login procedures to enhance security. Multi-factor authentication is a crucial element of contemporary security practices, offering an extra layer of protection beyond conventional username and password combinations. By necessitating multiple forms of verification, MFA markedly diminishes the risk of unauthorized access and enhances overall system security.

The authors discuss various MFA methods and their effectiveness in different contexts, emphasizing how they can be applied to strengthen login security. They outline the technical aspects of implementing MFA, including the selection of authentication factors including knowledge-based (passwords), possession-based (security tokens or mobile devices), and inherence-based (biometrics). Their paper also covers the practical challenges and considerations involved in deploying MFA solutions, including user experience, system compatibility, and the balance between security and convenience. The study provides insights into how MFA can be effectively utilized to protect sensitive information and systems from potential threats. ALSaleem and Alshoshan's work contributes to the field by offering a detailed examination of MFA applications in system login processes, highlighting its importance in contemporary cybersecurity practices and its role in safeguarding against unauthorized access.

[9] A comprehensive survey of multi-factor authentication. (MFA) methods within the context of cyber-physical systems (CPS). In their survey, the authors explore the implementation and effectiveness of MFA in the realm of cyber-physical systems, which integrate computational and physical processes. As these systems become increasingly complex and interconnected, ensuring their security against unauthorized access and cyber threats is crucial. The paper offers a detailed review of various MFA techniques and their application to CPS, emphasizing their importance in enhancing system security. MFA methods typically combine multiple forms of verification—such as knowledge of passwords, possession of security tokens or mobile devices, and identity of the user (biometric data) (biometric traits)—to strengthen authentication processes. The authors analyze the current state of MFA technologies, discussing their benefits, limitations, and suitability for.

Rokhimov, Hui, Al-Absi, Lee, and Sain's survey contributes valuable knowledge to the field of cybersecurity for cyber-physical systems, highlighting the critical role of multi-factor authentication in safeguarding complex and sensitive systems. Their work underscores the need for robust authentication mechanisms to address evolving security challenges in

[10] "Your Password Is Music to My Ears: Cloud Based Authentication Using Sound" by A. Phipps, K. Ouazzane, and V. Vassilev, presented at the 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), explores an innovative approach to authentication using sound-based methods in cloud environments. The authors propose a novel authentication system that leverages audio signals for secure access to cloud-based services.

The study addresses the growing need for secure and user-friendly authentication methods in cloud computing. Traditional authentication methods, such as passwords and tokens, are often vulnerable to various security threats. In contrast, sound-based authentication offers a unique alternative by using sound patterns as a form of verification. The paper details how sound waves can be utilized to generate unique authentication credentials, providing both security and convenience.

The authors describe the technical aspects of their proposed system, including how audio signals are captured, processed, and analyzed to verify user identities. They discuss the potential benefits of using sound for authentication, such as reduced susceptibility to common attacks and an intuitive user experience. The paper also considers the challenges and limitations of sound-based authentication, including issues related to audio quality and environmental noise.

III. METHODOLOGY

3.1 Proposed system:

The proposed system utilizes a comprehensive multi-step approach to bolster security and enhance user verification. Initially, users must establish a secure username and password. When a user accesses the system by clicking on a URL, the system captures the unique device ID of the user's device. This feature is particularly suited for applications demanding high security standards, providing a robust solution for user registration and data protection.

During the initial registration phase, users must establish an account by providing a username, password, email address, and a live image capture. Once all required details are entered and the submit button is clicked, the system

generates a unique file incorporating the username, device ID, and the first three digits of the password. This data is encrypted using a hashing algorithm before being transmitted to the database (DB) for secure storage.

At the login stage, users enter their username and password and then click the "log in" button. The system employs the same encryption process by combining the username, device ID, and the first three digits of the password. This encrypted data is sent to the database, where it is validated against the stored records. If the username and password are correct, the system then verifies the encrypted file data. If the data matches, access to the system is granted to the user.

In cases where the username and password are correct, but the device ID does not match, the system prompts for a live image capture. The live image is compared against the previously captured image. If the live image matches, access is granted. Otherwise, the system denies access to protect against unauthorized logins. This mechanism ensures that even if an attacker has obtained the correct username and password, they would still need the appropriate device and a live image to gain access.

The proposed system is designed to handle applications that require stringent access control and data protection. By implementing this multi-phase methodology, it ensures the integrity and security of user credentials. This approach effectively mitigates the risk of attackers misusing stolen credentials, as it combines multiple layers of verification, including device-specific and biometric checks.

The accompanying figure illustrates the data flow involved in user authentication. It shows how encrypted data is transmitted to verify user identity and allow login only if the data matches the records in the database. This detailed process highlights the system's capability to ensure secure and reliable user verification, safeguarding against unauthorized access and protecting sensitive information from potential breaches.

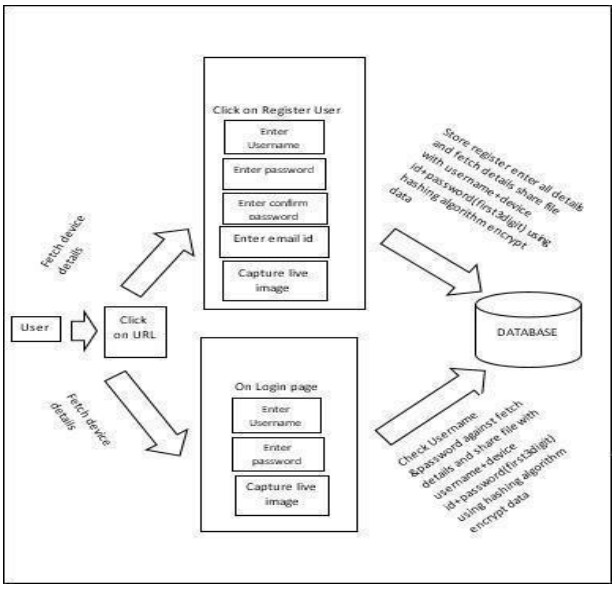


Figure 1. Dataflow of the user authenticate system

The figure above illustrates the process of data flow for authenticating user identity, enabling login only if the data matches the records stored in the database.

3.2 Registration Process:

To begin using the application, users must first complete the registration process. This involves gathering necessary user information and verifying its validity through the system.

START

- Click on URL: The system fetches the device ID.
- Click on Register User: Initiates the registration process.
- Enter Username: User provides a username.
- Enter Password: User sets a password.
- Enter Confirm Password: User confirms the password.
- Enter Email ID: User provides an email address.
- Click on Submit Button: Finalizes the registration submission.
- Password Validation Verify that the password and confirm password fields are identical. If they do not, prompt the user to correct them.

- Successful Registration: If passwords match, the system generates a file containing the username, device ID, and the first three digits of the password, encrypted using a hashing algorithm, and then stores this information in the database.

3.3 Login Process:

For registered users, the login process allows access if the credentials are correct. Invalid credentials trigger an error message.

START

- Click on URL: Fetches system details.
- Enter Username: User inputs their username.
- Enter Password: User inputs their password.
- Click on Submit Button: The system shares a file containing the username, device ID, and the first three digits of the password, encrypted using a hashing algorithm, and sends it to the database.
- The system verifies whether the password corresponds to the provided username. File Details Verification: If the password matches, the system verifies the file details.
- Error Handling: If the password does if the passwords do not match, an error message is displayed.
- Access Approval: If the file details match, the user is allowed to log in.
- Device Check: If a different device is used, the system prompts for a live image capture. If the live image, along with the username, password, and device ID, matches, access is granted.
- Access Denied: If details in the database do not match, access is blocked; otherwise, the user is allowed to log in.

3.4 Facial Recognition:

Facial recognition technology matches live images with previously captured images. Developed in the 1960s by pioneers such as Woody Bledsoe, Helen Chan Wolf, and Charles Bison, this technique enables computers to recognize human faces. Integrating facial recognition into Multi-Factor Authentication (MFA) significantly enhances both security and user experience.

After successful username and password authentication, users are prompted for a live facial recognition scan via the device's camera. This scan captures unique facial features, which are then compared to a stored facial template associated with the user's account.

Facial recognition is a powerful addition to traditional MFA offers enhanced security and an improved user experience by adding an extra layer of protection beyond standard login and password checks. This approach enhances security by requiring multiple forms of Confirmation. Forms of authentication, increasing the difficulty for unauthorized individuals to obtain access. This method greatly lowers the possibility of unwanted access.

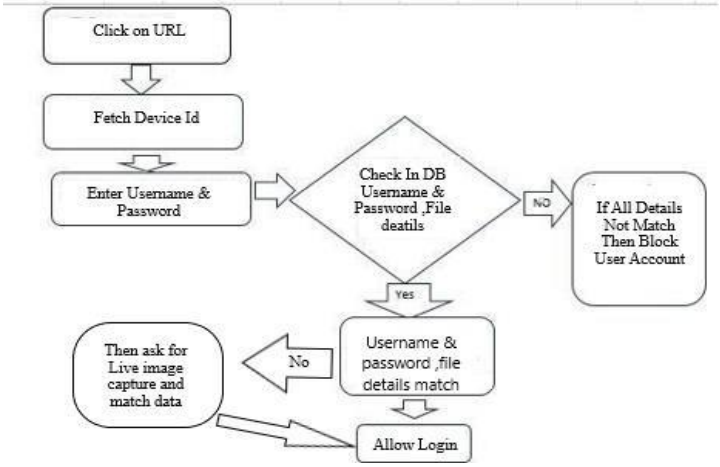


Fig2. Flowchart diagram of application

The technology captures real-time facial features, including the positions of the eyes, nose, and mouth, and compares them to the stored facial template. Ensuring robust security and user privacy involves using hashing techniques to prevent unauthorized access and offering alternative authentication methods for users who encounter difficulties with facial recognition.

The figure illustrates a secure user registration and login system that integrates device authentication, user data storage, and additional safety measures. When a user clicks on the URL to begin registration, the system retrieves the device ID, providing a unique identifier for the user's device. This device ID ensures that only authorized devices can access the application.

During registration, users must input their username, password, confirm their password, provide an email address, and capture a live image using the device's webcam. This multi-step registration process enhances security by collecting critical user information and biometric data. Once the live image is captured, the user can review it for accuracy before finalizing the registration.

When the user clicks the "Submit" button, the application securely stores all submitted information, including the device ID, in a database. Additionally, the system creates and shares a file containing a unique identifier derived from the username, device ID, and a portion of the hashed password (e.g., the first three digits). This file ensures that the user's registration and login information are securely linked.

For added security, the application cross-verifies the details in the shared file against the current user's data and device. If the file details match, the user progresses to the next step, which involves facial recognition. This biometric authentication phase verifies that the user attempting to log in matches the live image captured during registration.

This final security check ensures that only authorized individuals are able to access the application, maintaining high levels of security and protecting user data from unauthorized access.

IV. ARCHITECTURE DESCRIPTION

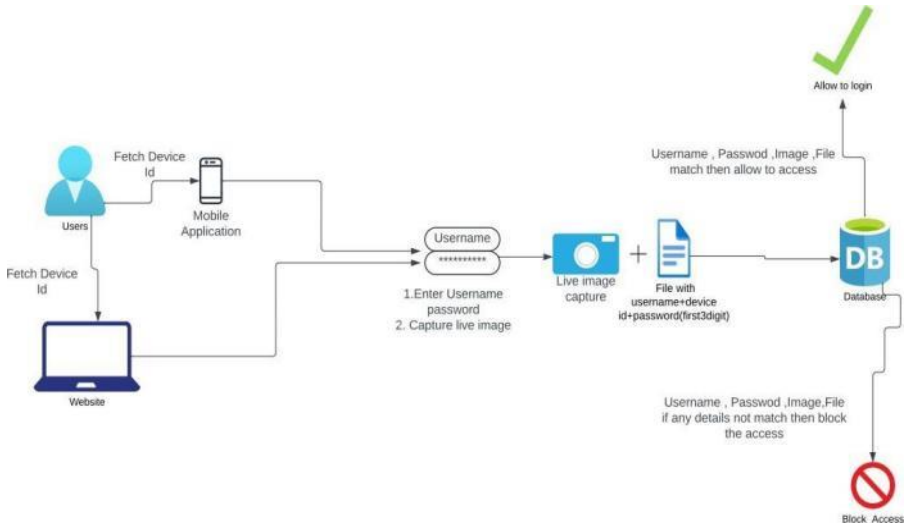


Fig3. Architecture diagram of application

- Frontend: The frontend user interface (UI) is designed to accept registration and login credentials. This interface is accessible via a webpage or mobile device, allowing users to interact with the system and input their information.
- Backend: The backend is responsible for connecting to the database to validate user data and manage interactions. It ensures secure handling of user details, including data transfer and validation processes, to maintain data integrity and confidentiality.
- Database: The database securely stores user information, including a secret key composed of the username, password, and the first three digits of the device ID. This stored data is protected to prevent unauthorized access.
- User Authentication Process: To ensure high security, the system verifies usernames and passwords against the database. The authentication process is fortified with live image capture and a hashing algorithm to provide an additional layer of security, safeguarding user data and confirming identity.
- Device ID Acquisition: When a user clicks on the URL, the system retrieves the device ID, providing a unique identifier for the user's device. This device ID acts as a security key in the authentication process, enhancing device-specific access control.
- This By using biometric data to confirm the user's identity, this feature improves security by making sure that only authorized users can access the system.

- .by comparing the live image with previously stored data. Security Feature: The system employs a robust hashing algorithm to encrypt and decrypt user data, safeguarding it from unauthorized access. This encryption ensures that user information stored in the database remains secure and protected.
- Access Control: Access to the system is granted only if all provided details match those stored in the database. If any discrepancies are found, the system blocks access to prevent unauthorized entry, maintaining the security and integrity of the application.

V. IMPLEMENTATION

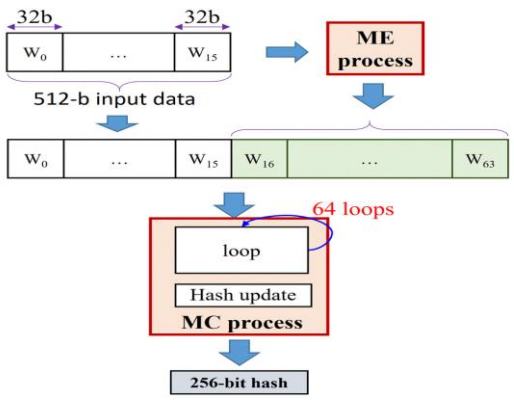
5.1 Secure Multi-Factor Authentication with Hashing Algorithm

Overview

This multi-factor authentication (MFA) algorithm enhances security by using a combination of device ID, password, and biometric verification. It employs SHA-256 hashing to securely process and store user credentials.

Key Components

- Hashing Algorithm: SHA-256 (256-bit hash)
- Authentication Factors:
  - Device ID
  - Password
  - Biometric Data (Face Recognition)
- Algorithm Steps



- User Registration:
  - Input: Username, Password, Device ID
  - Process:
  - Hash the password:

$$Hashpassword = SHA - 256(Password)$$

  - Concatenate hashed password with Device ID and hash again:

$$Final\_Hash = SHA - 256(Hashpassword + Device\ ID)$$

  - Store Username, Device ID, and Final Hash in the database.
- User Login:
  - Input: Username, Password, Live Image
- Process:
  - Retrieve stored Device ID and Final Hash for the given Username.
  - Hash the provided password:

$$Hashprovided = SHA - 256(Password)$$

  - Concede hashed passwords with ID:

$$Final\_Hashcomputed = SHA - 256(Hashprovided + Device\ ID)$$

  - 4. Compare computed Final Hash with stored Final Hash.
  - 5. If hashes match, perform allow to access applications
  - 6. If Hash not match then ask to capture live image and verify with stored biometric data. If matched, grant access; otherwise, deny access.

- Device ID and Image Verification:
  - Input: Live Image, Device ID
  - Process:

$$Verify\ live\ image\ using\ facial\ recognition: Biometric\_Match = Facial\_Recognition(Live\ Image, Stored\ Image)$$

- Verify Device ID:

$$Device\_ID\_Match = (Current\ Device\ ID == Stored\ Device\ ID)$$

- If both biometric and device ID match, grant access.

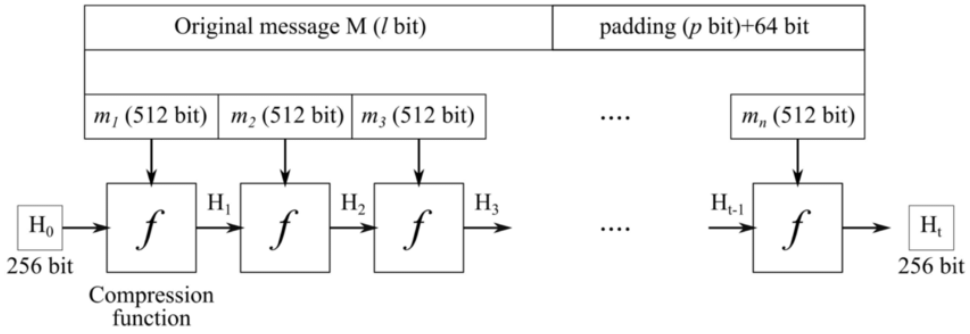


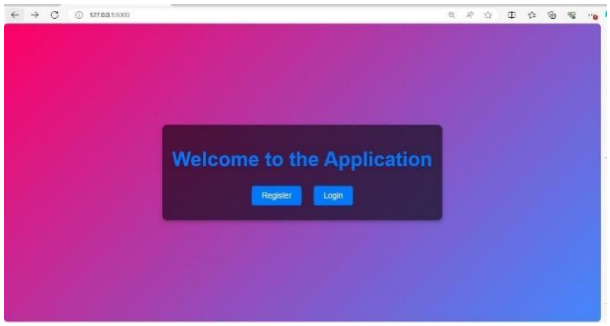
Figure2. Generation-of-hash-value-in-SHA-256

Summary

This algorithm ensures secure user authentication through:
- SHA-256 hashing for password and device ID.
- A combination of device ID, hashed password, and biometric data for multi-factor authentication.
- Protection against unauthorized access and cyber-attacks by securely handling and verifying user credentials.

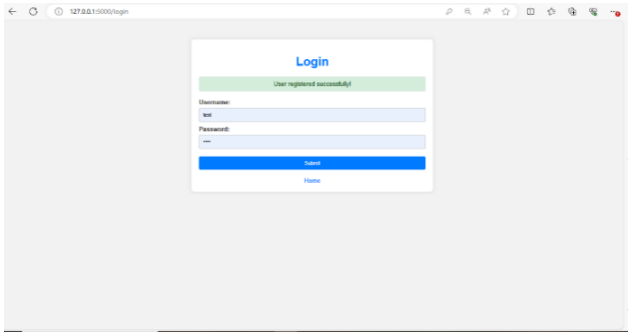
VI. RESULT

Home: This is the project flow to implement the security on login through multiple authentication on multiple user system IP ID'S.

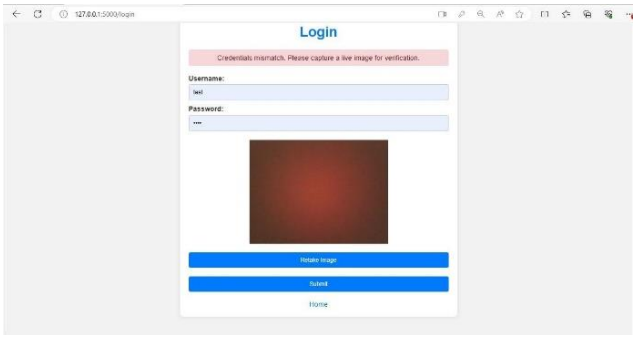


Register Page: The user need to be register with providing their details like username, email, password, ects.

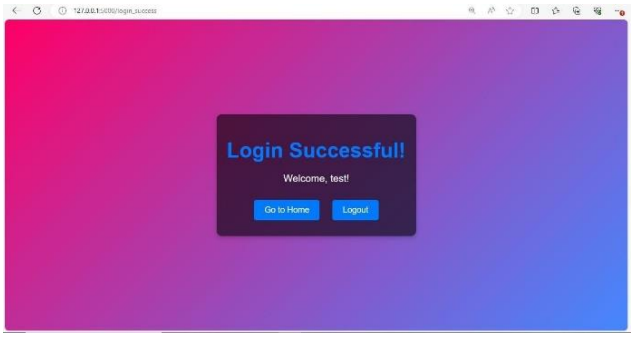
Login: After Registration the user can login using their valid credentials. And if Device id is used by the users then it should be ask to live capture the image.



Another Factor for Login: This is the face recognition to login the user securely. If the multiple times fail to login that user system IP will block automatically.



Login Successfully: The user can login successfully if the user credentials were correct.



VII. FUTURE WORK

Authentication applications are continually evolving to enhance security. Future research is focusing on advanced biometric identification methods, such as retina scans, voice recognition, and behavioral biometrics. Expanding the range of biometric identifiers can improve both security and user convenience. Additionally, advancements in machine learning and artificial intelligence can improve threat detection and prevention. Allowing systems to identify and block unauthorized access while adapting to new threats. Future developments should prioritize user experience and education, balancing stringent security measures with ease of use. As technology advances, the goal is to simplify the authentication process for authorized users while maintaining robust security.

VIII. CONCLUSION

In our research on multi-factor authentication (MFA), we have developed a new technique that enhances the security of the authentication process. This approach is more robust compared to previous methods and addresses the issue of hackers exploiting various systems to breach applications. By incorporating device ID checks, our system can distinguish between authorized users and potential intruders. Users authenticate using a combination of face recognition, passwords, and device IDs. Our proposed system employs three distinct authentication methods during the registration process, leveraging the uniqueness of device IDs to bolster security. The multi-factor authentication ensures that users complete the authorization process securely. Overall, our system demonstrates the safety of user authentication through its varied security techniques, which include single, two-factor, and multi-factor authentication.

REFERENCES

[1] Y. Nogia, S. Singh and V. Tyagi, "Multifactor Authentication Schemes for Multiserver Based Wireless Application: A Review," 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2023, pp. 196- 201, doi:10.1109/ICSCCC58608.2023.10177011.

[2] H. Alamleh, A. A. S. AlQahtani and B. Al Smadi, "Secure Mobile Payment Architecture Enabling Multi-factor Authentication," 2023 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 2023, pp. 19-24, doi: 10.1109/SIEDS58326.2023.10137778.

[3] Z. S. Alattar, T. Abbes and F. Zerai, "Smartphone-key: Hands-free two-factor authentication for voice-controlled devices using Wi-Fi location," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2023.3245080.

[4] J. Liu, K. Cui, X. Zou, J. Han, F. Lin and K. Ren, "Reliable MultiFactor User Authentication With One Single Finger Swipe," in IEEE/ACM Transactions on Networking, vol. 31, no. 3, pp. 1117- 1131, June 2023, doi: 10.1109/TNET.2022.3208002.

[5] R. Achary and C. J. Shelke, "Fraud Detection in Banking Transactions Using Machine Learning," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 221-226, doi:10.1109/IITCEE57236.2023.10091067.

[6] L.Déncs-Fazakas, E. Kail and R. Fleiner, "Two-factor, continuous authentication framework for multi-site large enterprises," 2020 IEEE 20th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 2020, pp. 173- 178, doi:10.1109/CINTI51262.2020.9305817.

[7] M.A. Hassan and Z. Shukur, "A Secure Multi Factor User Authentication Framework for Electronic Payment System," 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 2021, pp. 1-6, doi: 10.1109/CRC50527.2021.9392564.

[8] B.O. ALSaleem and A. I. Alshoshan, "Multi-Factor Authentication to Systems Login," 2021 National Computing Colleges Conference (NCCC), TaiBibliographyf, Saudi Arabia, 2021, pp. 1-4, doi: 10.1109/NCCC49330.2021.9428806.

[9] S.Ibrokhimov, K. L. Hui, A. Abdulhakim Al-Absi, h. j. lee and M. Sain, "Multi-Factor Authentication in Cyber Physical System: A State of Art Survey," 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South),2019, pp. 279-284, doi: 10.23919/ICACT.2019.8701960.

[10] A.Phipps, K. Ouazzane and V. Vassilev, "Your Password Is Music To My Ears: CloudBased Authentication Using Sound," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2021, pp. 227-232, doi:10.1109/Confluence51648.2021.9377126