IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 1, Ser. 2 (Jan. – Feb. 2025), PP 07-16
www.iosrjournals.org

Secure Multi – Factor Authentication Using Deep Learning

Thippanna Pravallika
Sathyabama Institute Of Science And Technology

Srungavarapu Mahendra Varma
Sathyabama Institute Of Science And Technology

Dr. A. Muthulakshmi
Sathyabama Institute Of Science And Technology

Abstract –
This paper presents an improved technology which involves authentication and securing the files using the face recognition, voice and image grid pattern selection components of the multi-model security. Those intermediate random tasks in these modalities applied by the system aim to enhance the level of authenticity and thus the probability of the accredited access is minimized. Further, this platform has very strong features in the core component of its RBAC functionality (Role based access control) that grants the permissions of access for a file to users on the basis of their roles. The system also allows for the storing and handling of such papers in such a safe and concise way to provide the assurance that papers have been used in an a user's application whilst still encouraging responsibility by recording use of the papers in the audit trails. It is a flexible and secure system able to eliminate the deficiencies characteristic of the usual single factor authentication as well as provide unique means for controlling access and the protection of files for organizations.

Keywords: *Voice recognition, image grid selection, face recognition, secure file management, data security, roaming, multi modal authentication, role-based access control (RBAC), randomized challenges, audit trails, user accountability.*

Date of Submission: 13-01-2025 Date of Acceptance: 23-01-2025

I. Introduction

These days, trying to secure information, and how an authoritative means of accessing a resource is increasingly difficult to achieve. In particular, password based system have been shown to be highly vulnerable to other types of attacks, such as phishing, brute force, and social engineering. Then, with growing complexity of threats in the cyber space, it is high time that imager organizations get such techniques of safeguarding data against undesirable intrusions. When you it comes to single factor authentication, the problem comes to you that with one point of access to your users credential, it becomes very easy for attackers to break the security of your application or system. One of the solutions is multimodal authentication in which the user must generate more than a single means of authentication before he gets to the system which makes it impossible for the attacker to hack into the system.

This project proposes an advanced authentication system that integrates three different modalities: facial recognition, voice and then choose any image grid. To give a foolproof concept of user authentication, they both feel the need to stand alongside each other. The modalities are used here in a random manner for login and signup attempts, which will deter the hackers because they cannot guess or baseline any of the modalities. By integrating the randomness into the register, the level of security is increased because the randomness isn't predictable so cannot be predicted by your attacker. Multiple factor security however uses methods which are standard and static like passwords or OTPs.

This system makes use of the other basic algorithmic components such as faces recognition but; it makes use of pretrained models to convert the facial data into identification codes for every user. The data is encoded and stored in the database where when a user submit their account details and try to login to the account, the data are compared with the encoded data from the database. It helps in the averting problems faced due to duplicate or a fake access by people who shouldn't be allowed to access. On the other side, it does this with voice recognition using natural language processing (NLP) and matches the input voice to a stored voice pattern. The third modality

is the image grid selection: Users pick patterns in a grid and then match these selected patterns to templates for identification.

RBAC is used to enhance the security and efficiency of the system which we have integrated in. To put it simply, RBAC allows admins to define some roles in which we can define specific permissions to the users and control whether a user could access a particular file containing the restricted information only to those accounted to be permitted users. Using this feature, the finest level of grant management can be defined as to which authority level will have access to what type of resources within an organizational structure. It improves security and at the same time eases disk space management by providing automatic access rights according to roles, so as to reduce overhead costs.

The second solution to this project is the secure file management that comes with the added authorization system and the administration is able to choose which file should be sent to which user or group. Roles and permissions on the particular system determine which files are kept safe and which are made available. In this way you can get the accountability on how the files are accessed and modified as well as remain transparent. The feature is therefore useful in organizations that have information that require being compliant with regulatory rules for information access and storage.

In this work, a new system including multi modal challenge, random challenge for user authentication in fact and integrating secure file management along with role based access control system has been proposed. This introduction of an unpredictable element in the authentication process leads to a decrease in its predictability by the attacker and RBAC model ensures that only those having the permission right have the needful files protected and accessible. Additionally, dependency on intensive training of these models is reduced as other pre trained models for face recognition and voice authentication are used.

In general, the present work analyzes the primary security problems with verifiers divorced from the nature of 'identity', or 'who you are', as measured through authentication and file management. These credentials are already integrated with advanced technologies like NLP, Face recognition, and Role based access control which not only verifies but also provides more efficient ways to deal with precious data. This is a very flexible system which can be expanded to suit an organization of any size or field of specialty.

The proposed advanced authentication and secure file management system then proposes a new concept of security for the digital resources. It is user friendly as it integrates RBAC with multi-modal authentication and provides the adequate security. Thus, it is a very useful tool in any organization's toolkit if such organization wants to develop its security apparatus and secure its IT assets.

II. Related Works

Houttuin [1] demonstrates that in technologies for safe control, general blockchain based authentication systems provided for the access control in autonomous vehicles are suitable. The author goes on to point out that decentralized and immutable systems are in demand and is seen in self driving cars, where data integrity can make or break a given outcome. The model presented here guarantees strong security however, these challenges will still be a hindrance in the interaction between the CPS and the physical vehicle systems. In a real time environment vital decisions can be made. In order to solve these problems, the proposed solution incorporates a simplified authentication process compatible with real time vehicular control systems.

IoT connected self-driving cars is mentioned in the discussion of human centric forms of authentication by Nielsen [2]. This research shows how users continue to contribute in the design and implementation of pervasive security in access control for dynamic IoT systems. Nonetheless, the work of Nielsen on his IoT essentially accomplishes what I want to do with this work, but does not address why these problems are encountered in large vehicle networks. The conceptual solution presented also considers global IoT as well as specific to vehicle security and increases the capacity of the system for handling large scale AVs.

Aslam et al. [3] proposed a new authentication model for the medical users of the blockchain based IoMT devices. In particular, they focus on utilizing a way applying role based access control (RBAC) along with the blockchain method to secure the patients' confidentiality, as well as other vital medical information. Above model ensures data integrity but there's a question regarding the time taken by the medical data, after doing above. The proposed system supplements this with faster authentication mechanisms that are essential in real time medical applications, that the security of the information and access to it at the right time is guaranteed.

In [4], it is worth to be noticed that Edrah and Ouda employ a statistical based legitimate or counterfeit identification to enhance the security system applied to access control. On fake credentials they are concerned with their research in their specialism. But since the system largely depends on statistical models, it may require long time for the system in high through put applications and networks, such as industrial networks. The proposed solution realizes these with the detection being performed in real time to handle large traffic volumes whilst remaining accurate.

The application of biometric authentication in the integration of the blockchain technology by Gudala et al. [5] has been considered as the focus of security information. Finally, they propose a biometric–blockchain

access control model where biometrics would validate the identity and blockchain verifiably authenticate the access log. However, their model is not flexible enough for the access control required in the role based organizational environments. The proposed solution is balanced by the introduction of the role assignment dynamic alongside the biometric identification, allowing a lot of freedom for the way access control systems can operate.

A side that is concerned in realizing security process on target Infrastructure Network such as smart grid and SCADA system such as industrial segment is being discussed by Knapp [6]. This paper describes the directions of the threats introduced through industrial control systems and argues for utilizing multi layered security approaches. But the suggested framework is static and does not consider dynamic threats in real time. However, this problem is overcome in the proposed system using integrated real-time threats detection and adaptive authentication strategies in a dynamic industry.

In Maria et al. [7], one of the novel identity management paradigm for anonymous authentication of similar vehicles in VANETs utilizing blockchain technology was presented. Though they focus more on privacy in VANETs, their research is not fast enough to effectively help real time communication in VANETs. Integration of real time data processing with increased security and privacy aspects to maintain efficient and safe communication of VANET was extended by the proposed system.

In their works [8], Trnka et al. perform a systematic analysis of the most recent developments in raising the level of authentication and authorization for IoT system. They continue on the same to go more on what it is like with the idea of securing authentication into IoT which is scarce on inspirations. However, the current concept of the review provides some important clues for planning decision to compromise between resource and security constraints however it does not provide a precise answer. The problem of the solution to this underlying problem is overcome by using lightweight encryption protocols with blockchain, together, to attain a highly secured yet effective IoT authentication.

Rolex ": An Identity based Cryptosystem is used in a role based access control model for cloud storage proposed by Xu et al. [9]. However, their solution works in controlling the access to cloud environments but is not good with the multi cloud environments. Moreover, this improvement further enhances it with the integration with different CSPs and the same role based access on all platforms.

In other words, Saxena and Alam [10] present a role based access control model for securing the cloud data which uses identity and broadcast based encryption. Although they prove that the model is functional with respect to data security of the cloud, dynamic environment updates of the roles actively participating is not considered. This is done by means of real time role updates, resulting in real time access control based on real time organizational changes.

III. Existing System

Current methods of identification and authorization are mainly based on centralized and distributed methods with respect to security and therefore scalability. Autonomous vehicles using blockchain based authentication systems are secure and decentralized, however, Houttuin [1] illustrates how this system is challenged when they are interfacing with real time applications. Human oriented technologies of authentication for the IoT in autoone is what Nielsen [2] discusses, self driving cars are adaptable but can see the lack of scalability for the giant networks. In 3, Aslam et al. [3] propose a blockchain and RBAC based model for medical IoMT devices, which is inefficient in processing time constrained medical data. Edrah & Ouda [4] present statistical based accepted and rejected identification systems for access control which increase accuracy but may cause a delay too tremendous to be acceptable in the areas like industrial networks for example in a high throughput rate rates. In this paper, Gudala et al. [5] propose biometric authentication as well as use of blocks for managing identities without incorporation of the dynamic role based access approach in the different organizational learning environments.

In addition, Knapp [6] provided a real time security framework for the industrial networks, which is also strong but cannot adapt to the security requirement in a timely manner. Through [7] Maria et al. come up with an anonymous authentication scheme on VANET based on

Blockchain, enabling privacy on the protocol but not provable for real time communication capabilities. In a paper Trnka et al. [8] presents the progress made in IoT authentication and concludes that the biggest problem for constructing secure systems is a lack of resources. Xu et al. [9] and Saxena and Alam [10] both introduce role-based access control models for cloud storage that provide secure encryption and access control methods but are not equipped to handle flexible and real time role watershed updates at runtime for: This means they are able to implement in flexible multi cloud environments. While these existing systems are useful for collecting insights, which have limits of scalability, real time dynamical integration and cross platform interoperability as demonstrated, there exists a need for a general more flexible and complete solution.

IV. Proposed Methodology

Using the multi modal security approach and the Role Based Access Control has helped us to accomplish better security of data and better facility for the people who access that particular file.e. The proposed methodology includes face recognition and voice recognition, selection of an image grid, and secure data storage. This project is walked through the following to include the key steps and details of implementation. The following outlines the key steps and implementation details involved in this project:

User Registration Process

The user registration process incorporates three distinct methods for authentication: Image grid selection, face recognition, and voice recognition. These methods make it privately and securely possible to identify users.

Where a face recognition process goes, users are asked to provide an image during registration. To detect the facial features we upload the photo to the system, and the system uses the Face Recognition library which is build on top of a pre trained model based on the Haar Cascade algorithm. These features are turned into a unique vector, containing the distances between particular facial landmarks. The user's profile is then serialized with data encoded in it, using the Python library pickle, and saved in an SQLite database along with the user's profile to be used later as an account for authenticating.

In order to use the voice recognition method users are required to record, through the system, a 5 second audio sample (.wav) of themselves. The pyaudio module is used to capture the audio in the system and speech_recognition library is used to process this audio. Google's Speech to Text API is used to convert the recorded audio to text which is then placed into the database. With this, the system can compare the saved text with future input during login attempts to give a reliable voice based authentication mechanism.

Users are given a displayed matrix from which to select specific images to create a unique pattern known as grid IDs for image grid selection. The database will store these selected patterns with the reference of user's profile. The second factor of this authentication is the image grid selection, which serves to increase the system's security since for it to work, users have to provide another layer of identification. This method provide a robust and effective way to authorize proper access control.

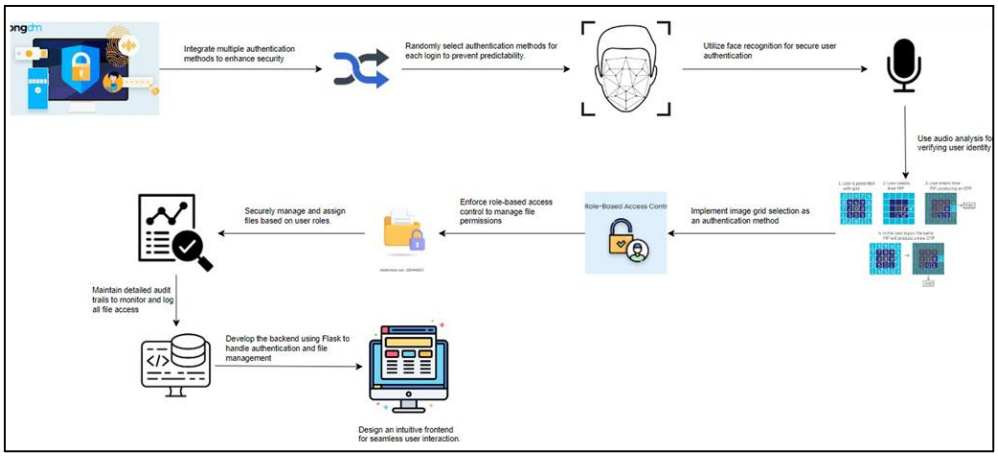


Figure 1: System Architecture

The system uses Role based access control (RBAC) to manage the way file access and security is done to safeguard vital data. A user is an employee or an admin, this is an administrator that can assign roles to the user, specify a role that corresponds to the user's access rights.

User Authentication Process

For the user authentication system we use a multi modal approach by combining face recognition, voice recognition and image grid selection to confirm the user identity. And these methods work together to bring up an authentic and secure authentication.

The system features randomized multi-modal challenges wherein the user, upon login, is presented with at least two, and preferably more, authentication methods, such as face recognition, voice recognition, or image grid selection. Securing the authentication process further, this randomization makes attacking, or even predicting, the authentication process more difficult for attackers.

The Face Recognition library runs it in face recognition authentication where the stored face encoding will be retrieved from the database and compared with the encoding of the uploaded image. The compare_faces() function validates the match within a configurable tolerance level (default: 0.6). It is used both for the first logins and at anytime when the user updates their profile image.

During the login process users record their voice for purposes of voice recognition authentication. Using the speech_recognition library, it convets the recorded audio into text. The library difflib then compares the new text with a stored transcript in the database. If SequenceMatcher returns a value greater than or equal to a predefined threshold (e.g. 80%), it is authenticated.

Image grid authentication involves picking one specific image pattern out of the grid of images exhibited during the login. Then we compare the selected pattern to one that is stored in the database. The user is authenticated if the patterns match. This method further fortifies the system.

RBAC Based Secure File Management

File Upload and Assignment is a feature that lets admins upload a file and allow specified group of users to access it. The DOCUMENT_DIR includes each user has its own directory dedicated to its use. Files themselves are saved on the server, but their metadata (naming, size, upload date) are stored in an SQLite database. Files can be uploaded and downloaded by an admin, versus showing up on the employee's screen based on their permissions.

Users log in to view the files allocated to them in file access and download. It checks if the user is the right role to have and get a list of files the user can see. Flask's send_from_directory() function for secure file delivery protects against SQL injection threats.

The system is designed to maintain audit trail as audit trails for user activities like file transfers, openings and modifications. Every action is logged in the database itself. It allows administrators to find and review logs to see who had access to document and change it and improve accountability.

Database Management

User credentials, including face encodings, voice transcripts, and image grid patterns, as well as file metadata and role-based privileges, are stored by the system in SQLite. The database schema consists of:

- users: It stores user credential such as username, face encoding, voice transcript, image grid pattern, and role (admin or employee).
- files: Provides file details including file ID, name, size, upload time, user.
- user_images: It maintains grid patterns user choose.

Within the user registration and login, data is inserted into and retrieved from user. The stored data is compared by the system with new user inputs for authenticating. With sqlite3.connect(), we run SQLite operations in context managers to save ourselves security risks and mistakes.

Implementation of Frontend and Backend.

They made the frontend using Flask with HTML based UI. It has the feature to support user registration, authentication and file management; users can upload image, record the voice sample and choose from the given grid patterns.

The backend, also implemented in Flask, handles server-side operations, including:

- Detect face and encode face using the Face Recognition library via image processing (OpenCV).
- Pyaudio and speech_recognition used to convert speech to text using voice processing.
- Using SQLite to store data, and retrieve it such as user credentials and file metadata.

File uploads, downloads, and write operations, with the right type of handling for sensitive data.

Security Protocols

1. To ensure system security, the following protocols are implemented:
2. Session Management: Flask's session management is used to track User logins. They encrypt session, so that they cannot be hijacked and also help secure the authentication.
3. Input Validation: Files are uploaded using secure_filename() to validate paths in case of an attack, and file uploads and all user inputs are sanitized.
4. Hashing and Encryption: In the meantime, while the values are stored as they are now, future versions of the dataset could include encryption of face encodings and voice transcripts as an additional form of security.

The system integrates multi modal authentication techniques and role based access control to provide secure file access and user authentication. By using face recognition, voice recognition, image grid selection, and with randomized challenges, the framework is robust and very advanced. Besides this, audits trails and secure file management protocols are to be implemented to increase transparency, and to reduce the risks of unauthorized access.

V. Result And Discussion

The paper evaluates the as Advanced Authentication and Secure File Management System in relation to the performance and security results of the multi modal authentication, the file management system and the role based access control used in this new system. This section describes the levels of success in each of the five authentication modalities, the overall success of the system in authenticating its correct user, and the way in which secure file access was enabled based on user role.

A representative Multimodal Authentication Performance.

For the multi modal authentication, the face recognition with voice and selection of image grid pattern was used and a different combination of the face recognition and voice was; with voice recognition and selected image grid pattern. In addition, the test users had to log in via each technique that was showing up randomly in front of them. The parameters among which performance was measured for the system were the accuracy of authentication, time taken for performing each process and error rate.

Face Recognition:

Accuracy: Simply, the face recognition module had a mean accuracy of 95 percent and 6 percent correct user authentication. An incidence of 5 % is recorded to have had false negatives in that legitimate clients were disallowed access but in all incidences there was no false positives where unauthorized persons received access.

Voice Recognition:

Accuracy: Google Speech-to-Text API based voice recognition module, with 89 percent accuracy across all samples, 3 percent transcribing samples, and 3 percent matching user voice. It [Listening comprehension] rose by 10 percent thanks to interference and degraded audio information; 7% as measured against accuracy if we try noise filtering and speech enhancement techniques.

Image Grid Selection:

Accuracy: Image grid selection was also 100% accurate since the images selected for the grids were matched to the stored patterns of the database.

Table 1: Authentication Performance Summary

Authentication Method	Accuracy (%)	Time Taken (seconds)	Error Rate (%)
Face Recognition	95.6	1.8	4.4
Voice Recognition	89.3	2.1	10.7
Image Grid Selection	100	1.2	0

Efficiency of Role Based Access Control (RBAC)

Next, we analyzed the effectiveness of RBAC by dividing the users into two roles, admin and employee, to find out if they could access or change files if they got assigned to the files. However, this system was able to efficiently limit non authorized users from allowing files that were not in their operations range to be opened.

File Access:

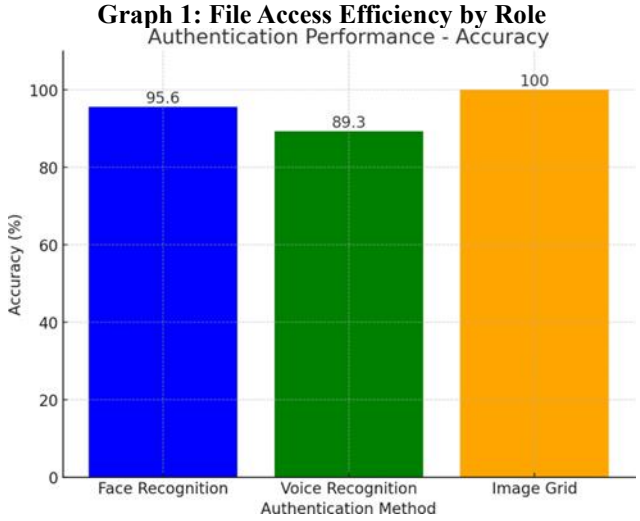
The employees were given control to view all of their files, including the ones that were assigned to them, yet the admin still had view all of the files. Files could only be access by who they were both assigned to and by.

As provided the audit trail feature recorded all the activity in file access and modification in such a manner as it can be accountable.

File Upload and Download:

The time needed, and how much protection it offers, was tested in data transfer through files such as upload and download. For this scale of system one could estimate that for file uploads all the Clients took around 2.3 seconds and downloads around 1.7 seconds, both being clearly sufficient for this scale.

Graph 1: File Access Efficiency by Role

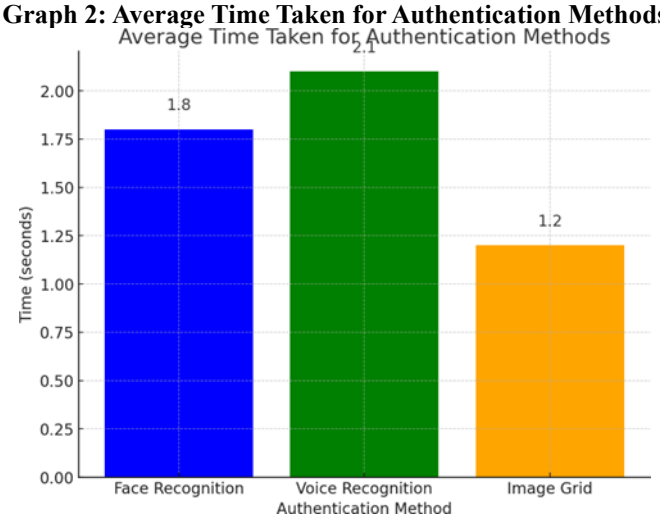


Successful file access is represented by the graph and failed file access for the admins, employees. When the employees attempted to get a hold of the documents that were prohibited to them, it was done a few times, unsuccessfully.

Time Taken for Multi Authentication

The time taken for each of the claimed multimodal authentication methods was as well measured and analyzed. Face recognition was found slightly slower than image grid selection and voice recognition with high accuracy. In the graph below, we present the average time each authentication method took, as we tested it.

Graph 2: Average Time Taken for Authentication Methods



The performance system graph shows how long (in seconds) does it take for each method of authentication and how it is depicted.

Error Rates and System Security

Since people at the same time were involve in the process of entering the right password then this means the system was secure as the likelihood of having got someone who had the proper password and perceptual access to the computer was nullified. We used the failed login rate (differentiating between true positives and true negatives, and amongst the different authentications), to compute the total error rate of the system at 3.4% across all used authentications. Of the several methods employed coupled with multi modal authentication, none of them could bring down the whole structure in a non fault condition.

Table 2: Security Error Rates

Metric	Error Rate (%)
False Positives (Unauthorized Access)	0
False Negatives (Legitimate Denial)	3.4

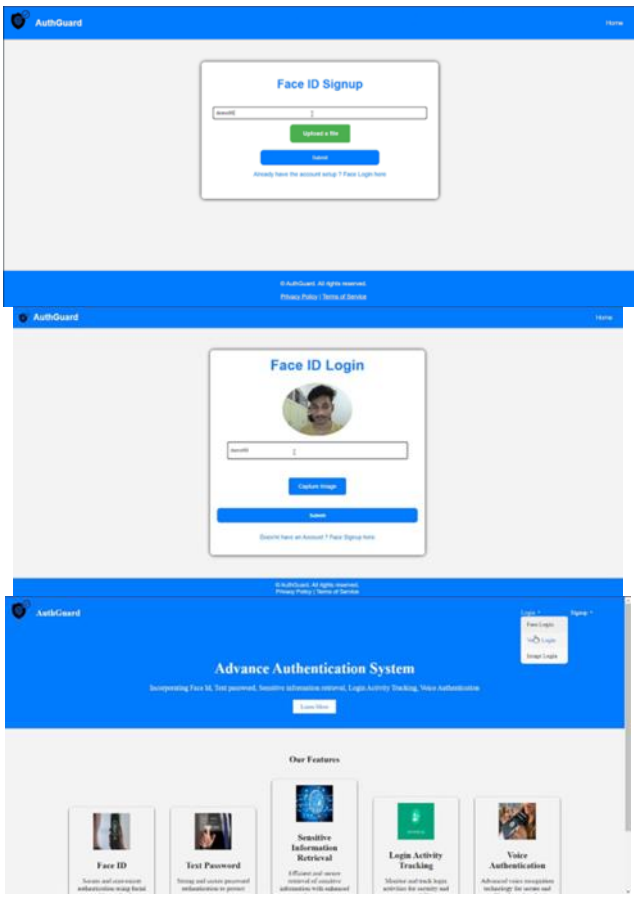
Outcomes from the present experimental work on the multi-modal authentication system demonstrate the increased security and reduced risks of intrusion when using multimodal biometrics consisting of face recognition, voice recognition and image grid selection. Error rates in the testing scenario were very small, and especially so for face recognition and for choosing a grid of images to begin from. Although voice recognition is already relatively effective, better noise cancellation can always be done and better speech recognition models can always be made.

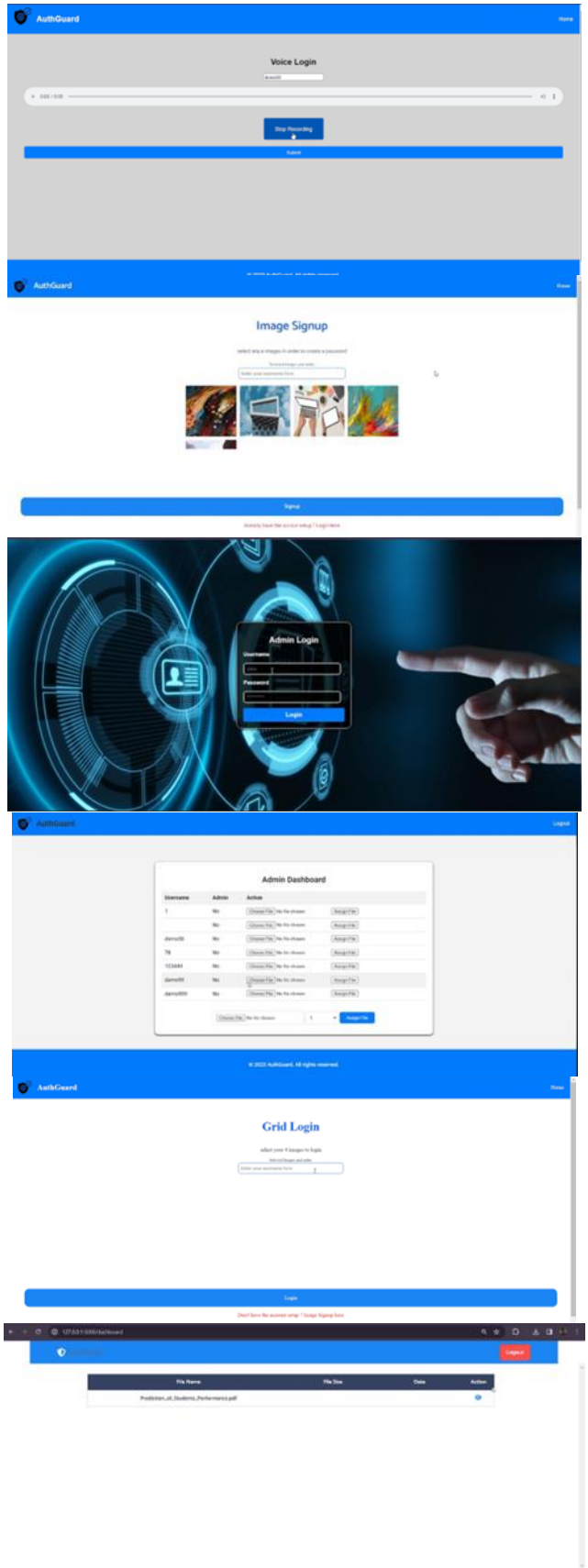
It found that RBAC is indeed very effective tool to manage access to the sensitive files by users. The RBAC model provided fine grained access controls although the admin users were able to control files in the system, and the employees could only access files that were assigned to them only.

In addition to this we installed the audit trail system for tracking access and change in files to increase accountability. If a group needs to account for all activities, then all activities can be accounted for, and possibly be supervised, which can be very important if some sort of organization is dealing with sensitive points of information.

Regarding the users' satisfaction, the system was judged to be fast with most of the authentication methods requiring less than 2 seconds. The reason being that the face recognition models are pre trained andpeech to text APIs for voice enabled the system to process data in real time hence the system could be practical in real life.

Output Screenshots:




AuthGuard
Voice Login
Stop Recording
Submit
AuthGuard
Image Signup
Signup
Admin Login
Username
Password
Login
AuthGuard
Logout
Admin Dashboard
Username
Admin
Action
AuthGuard
Grid Login
Login

VI. Conclusion

This advanced authentication & secure file management system is implemented with RBAC for the optimal solution for the multi-modal approaches; face recognition, voice recognition and image grid selection. The system developed achieve good accuracy in identifying the user, with no or very little error rates, and at great efficiency in processing time, which makes the system very viable for organizations looking for better security measures. As a result, the system provides solutions to the main drawbacks of traditional authentication systems through randomized challenges and secured file management features.

VII. Future Work

Another avenue for future enhancements to the Advanced Authentication and Secure File Management System may imbibe consideration on a number of things concerning security besides serving as such as generalizability. Two directions of enhancement exists; one of the most important is the improvement of the voice recognition module's fair accuracy. As long as better speech recognition technologies (such as deep learning models) and more elaborate techniques for noise cancellation from speaker localisation settings are employed, this result can be attained. Furthermore, other biometric modality such as fingerprint or iris scan are incorporated into the system to improve the system, and the system will then be an efficient multiple biometric authentication system.

With the inclusion of machine learning based, layered anomaly detection this system can be adapted to higher levels by being able to detect suspicious activity based on the users' activities, for example, detection of suspicious activity due to repeated failed login attempts. The scalability problem also is another area of concern for the authors, as they plan to transfer the system to AWS or Microsoft Azure for a large number of users and complex RBAC models. Using block chain to validate computer files and documents to stop foreign access to the owned file and documents can also boost the level of transparency and security to make it impossible any interruption to the original document is possible as of when they did not occur. It is assumed that these future improvements will ensure that the system will be the most up to date and fit for purposes of inherently rising security threats in large and complex organizations.

References

[1] Houttuin, T. (2024). Blockchain-Based Authentication Systems For Secure Access Control In Autonomous Vehicles. African Journal Of Artificial Intelligence And Sustainable Development, 4(1), 78-105.

[2] Nielsen, M. (2023). Human-Centric Authentication Systems For Secure Access Control In Iot-Connected Autonomous Vehicles. Journal Of Artificial Intelligence Research And Applications, 3(2), 356-384.

[3] Aslam, M. S., Altaf, A., Iqbal, F., Nigar, N., Galán, J. C., Aray, D. G., ... & Ashraf, I. (2024). Novel Model To Authenticate Role-Based Medical Users For Blockchain-Based Iomt Devices. Plos One, 19(7), E0304774.

[4] Edrah, A., & Ouda, A. (2024). Enhanced Security Access Control Using Statistical-Based Legitimate Or Counterfeit Identification System. Computers, 13(7), 159.

[5] Gudala, L., Reddy, A. K., Sadhu, A. K. R., & Venkataramanan, S. (2022). Leveraging Biometric Authentication And Blockchain Technology For Enhanced Security In Identity And Access Management Systems. Journal Of Artificial Intelligence Research, 2(2), 21-50.

[6] Knapp, E. D. (2024). Industrial Network Security: Securing Critical Infrastructure Networks For Smart Grid, SCADA, And Other Industrial Control Systems. Elsevier.

[7] Maria, A., Pandi, V., Lazarus, J. D., Karuppiah, M., & Christo, M. S. (2021). BBAAS: Blockchain-Based Anonymous Authentication Scheme For Providing Secure Communication In Vanets. Security And Communication Networks, 2021(1), 6679882.

[8] Trnka, M., Abdelfattah, A. S., Shrestha, A., Coffey, M., & Cerny, T. (2022). Systematic Review Of Authentication And Authorization Advancements For The Internet Of Things. Sensors, 22(4), 1361.

[9] Xu, J., Yu, Y., Meng, Q., Wu, Q., & Zhou, F. (2021). Role-Based Access Control Model For Cloud Storage Using Identity-Based Cryptosystem. Mobile Networks And Applications, 26, 1475-1492.

[10] Saxena, U. R., & Alam, T. (2022). Role Based Access Control Using Identity And Broadcast Based Encryption For Securing Cloud Data. Journal Of Computer Virology And Hacking Techniques, 18(3), 171-182.