

Adaptive Secure File System with Aes and Intrusion Detection Using Grassmann-Based Biometric Authentication

Mr. M. A. Amarnath¹, Dr. P. Chellammal², Swetha R³, Suganya P⁴, Sujeetha S⁵

¹ M.E, Computer Science and Engineering J.J College of Engineering and Technology Trichy. India.

^{2,3,4,5} Computer Science and Engineering J.J College of Engineering and Technology Trichy. India.

Abstract—The proposed Adaptive Secure File System improves the security of cloud data by using the integration of biometric security, encryption, and intrusion detection techniques. As the use of cloud storage facilities rises, the security risks of unauthorized access, data breach, and hacking of cloud data also increases. Therefore, to solve these security challenges, the proposed system uses facial biometric security, which relies on the Grassmann algorithm to validate the identity of users before allowing access to the cloud storage system. Once the identity of the user has been validated, the user can upload files to the cloud storage system. In order to improve the security of the cloud uploaded data, the proposed system uses the Advanced Encryption Standard (AES) to encrypt the uploaded files before storage in the cloud storage system. This way, the uploaded files remain secure even if the cloud storage system is hacked. The proposed Adaptive Secure File System also incorporates a real-time intrusion detection system to detect unauthorized access to the cloud storage system. The intrusion detection system monitors the login activities of the user to the cloud storage system, detecting unauthorized login activities to the cloud storage system.

Index Terms—Cloud Security, AES Encryption, Elliptic Curve Cryptography, Facial Recognition, Grassmann Manifold, Biometric Authentication, Intrusion Detection, Secure Cloud Storage, Data Protection, Cryptography, Cyber Threat Prevention.

I. INTRODUCTION

Cloud Computing has changed the way people store their data. The use of cloud computing for storage purposes is flexible. Nevertheless, the use of cloud computing services has led to a number of security issues. These issues include unauthorized use, data

breaches, and cyber attacks. Protecting cloud computing data is a major research topic [1]. Most cloud computing systems use conventional means of verifying user's identities. These means include the use of usernames and passwords. These two have been prone to attacks such as phishing attacks, brute force attacks, and stealing passwords. Therefore, there is a need for stronger means of verifying identities [2].

Another secure way to do this is the use of biometric authentication systems, which use unique physiological characteristics to identify users. Of all the various methods available for biometric authentication, the use of face recognition is the easiest and least intrusive. The proposed system would use the Grassmann-based feature extraction method to improve face recognition[3]. While the use of secure authentication systems would provide adequate security to the data stored in the cloud, the data would always remain vulnerable if encryption is not used. Encryption provides the best way to prevent unauthorized access to data and attacks at the server level [4].

For confidentiality, the system utilizes AES encryption for securing files, and the AES key is further protected using Elliptic Curve Cryptography (ECC), providing a dual-layer encryption mechanism. The files are double encrypted before they are stored in the system.[5]. Apart from the authentication and encryption of the data, the detection of unauthorized access attempts is also crucial. Most of the systems do not have the feature of intrusion detection to identify the suspicious activities in the system.[6].

The Adaptive Secure File System, which is being

proposed, incorporates the features of facial authentication, double AES encryption, and intrusion detection in an integrated manner. Only authenticated users can upload the files, and the data is encrypted in a secure manner before storing it [7].

Moreover, the integration of the biometric verification system doubles AEs encryption, and intrusion detection ensures that the data placed in the cloud is safe and secure. The facial recognition system prevents unauthorized access to the data, and the encryption of the data ensures that the files remain safe even if the encryption key is breached [8].

II. EXISTING SYSTEM

In the traditional cloud storage system, the security of the data is mainly achieved by username/password authentication, as well as single-layer encryption techniques. In the cloud storage environment, the majority of the cloud storage systems offer users the ability to store their files after successful username/password login using password authentication techniques. Although this approach has gained widespread use, it has become highly susceptible to various types of attacks, such as phishing, brute force, password stealing etc...

In existing systems, single layer encryption techniques have been used to secure the data, which means the data has been encrypted using symmetric or asymmetric encryption

techniques. Although the use of encryption techniques has achieved a certain level of security, the use of single-layer encryption has become inadequate if the encryption key has been exposed to attacks, as well as the use of complex cryptographic techniques.

Furthermore, the conventional cloud platforms usually do not have in-built biometric authentication tools. This means that without biometric verification tools such as face recognition and fingerprint scanning, the system is not in a position to ascertain that the actual user is the one accessing the system. Password and OTP verification tools only verify the credentials of the user and not the actual identity of the user trying to access the system. This leads to issues of trust on the part of the user and greatly

increases the chances of identity theft and unauthorized access to the system.

The second major limitation of conventional cloud platforms is the lack of real-time intrusion detection tools related to authentication failures. This means that without the ability to proactively monitor the system and identity unusual access patterns related to authentication failures, the system is not effectively respond to the threats in due course. This usually gives the attackers several changes to access the system without the system being able to prevent the intrusion in due course.

In essence, existing cloud storage solutions have weak authentication processes, single-layer encryption, weak monitoring processes, and unconnected security features. For instance, password-based authentication systems are highly vulnerable to phishing attacks and password cracking and theft. Moreover, cloud storage solutions have no real-time monitoring processes and unconnected security features. All these weak security features make existing cloud storage solutions highly vulnerable to sophisticated and emerging cyber threats and unauthorized data access.

III. PROPOSED SYSTEM

The proposed Adaptive Secure File System offers an integrated security model for cloud-based file management systems, incorporating biometric authentication, encryption, and intrusion detection systems as an integrated unified model. Unlike the traditional security model, it integrates the security features, making the security model more robust. It uses biometric authentication as the first security feature for identity verification before providing access to the cloud-based file management system. The user's facial image is captured during the registration process, allowing the biometric template to be created securely. The facial image is captured during the login process, allowing the biometric template to be matched for identity verification purposes.

To enhance the accuracy of recognition, the system uses the Grassmann-based feature extraction technique. The image of the face is preprocessed, resized, normalized, and cleaned of any noise before the Grassmann manifold technique is applied. This

technique converts the features of the face into a mathematical representation, allowing for the comparison of the face features, thus enhancing the accuracy of the matching. Once the similarity score is above the threshold, the user is granted access, thus authenticating the user. The authorization module is responsible for ensuring that the user is authorized before any file operation is performed, such as uploading, downloading, or sorting the files, all the authentication processes are logged for auditing purposes.

After the authentication process has been successfully carried out, the system allows the user to upload the file securely. Prior to the storage of any file in the cloud, the uploaded file is encrypted using the Advanced Encryption Standard (AES). The encryption process ensures that the file data is converted into different form, i.e., the file data is converted into ciphertext. This ensures that the information in the file remains confidential in case the cloud storage is compromised. The AES encryption key is further encrypted using Elliptic Curve Cryptography (ECC), ensuring secure key management and providing dual-layer encryption. After the encryption process has been finished, the file is sent to the cloud storage server. Only the encrypted data is stored in the cloud. The details related to the file, such as the upload time and the identification details of the user, are stored securely. In addition to this, the system incorporates a real-time intrusion detection and the alert System. If facial authentication fails, the system recognizes the attempt as an unauthorized access attempt. The image, time, and login details are recorded to analyze the security. The intrusion detection system monitors repeated failed login attempts and suspicious activities. Upon detecting potential threats, the system sends out alerts to notify the administrator, as well as immediately denying access to prevent the threat from using the system. The proposed system incorporates an adaptive, secure, and highly secure approach by using a combination of facial verification, AES encryption, cloud storage, and intrusion detection to secure the data in the cloud environment.

Moreover, the system is adaptable and expandable for use in situations where security demands change over time. The comprehensive framework is also efficient in coordinating the various security components involved in the system. Such as authentication module, encryption module, and intrusion detection module. This is a major advantage over existing systems since it eliminates any loopholes in security. With this advantage, the system is adaptable for use in academic institutions, businesses, as well as personal cloud storage systems.

IV. METHODOLOGY

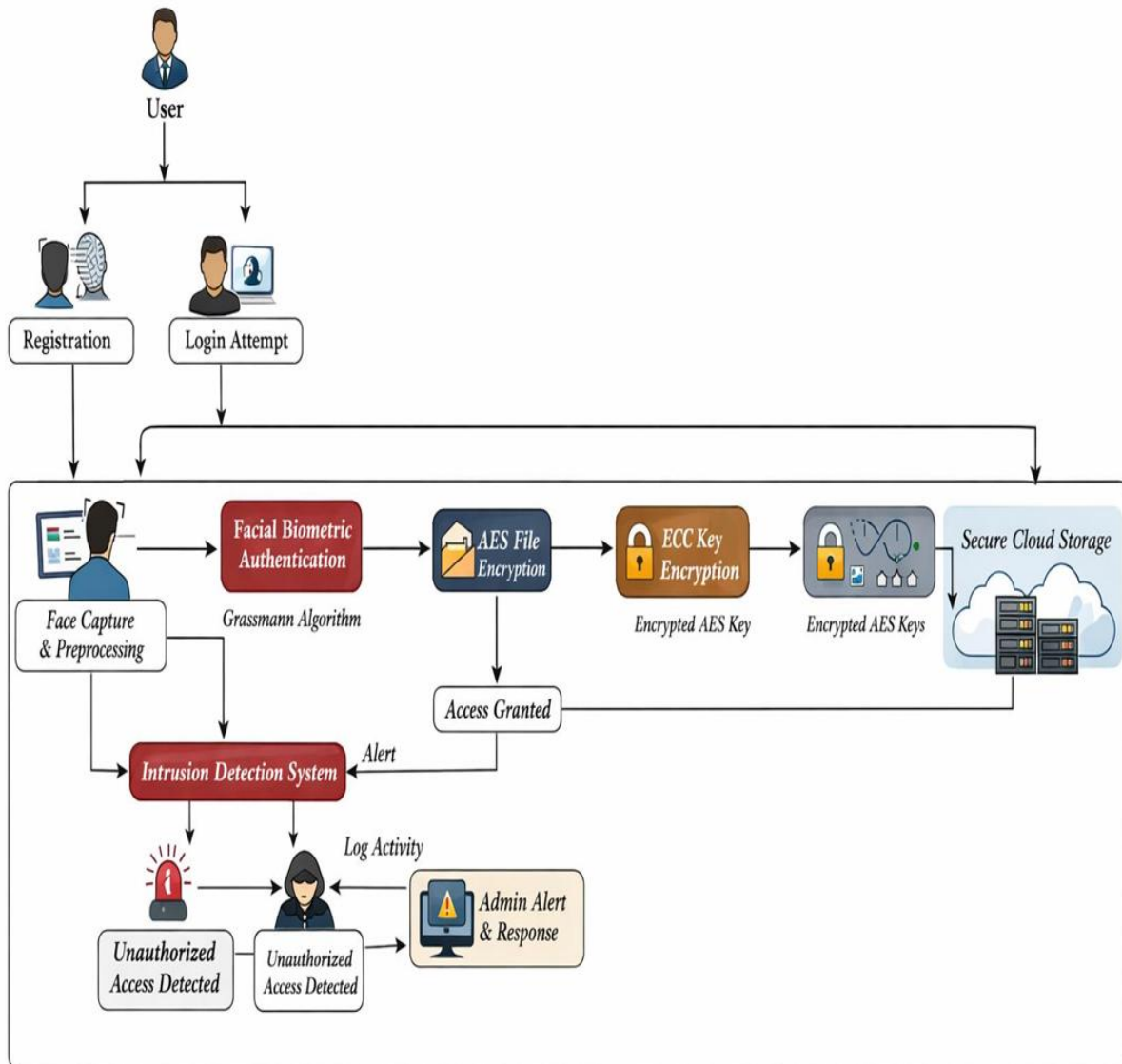
The proposed Adaptive Secure File System uses a specific and sequential methodology to achieve the goal of providing a safe and sound authentication system, along with the safe storage of information in an encrypted format. The entire process is divided into several phases, each responsible for a particular feature in the system.

A. User Registration and Biometric Data Acquisition

The user is required to register on the cloud platform by providing basic information such as username and email ID. During registration, the system captures the user's facial images through the device camera, where multiple images may be collected to improve accuracy and reliability. The captured images are then processed to generate a unique facial boundary template for future authentication and verification purposes. This template is securely stored in the cloud database to ensure fast and efficient identity validation during subsequent logins.

B. Image Preprocessing

The image of the face captured by the webcam goes through a series of image preprocessing techniques to improve the quality of the image. The image resizing, grayscale, normalization, removal of unwanted noises from the image are carried out in this phase. Additionally, the image detection of the face from the background takes place in this phase.



C. Grassmann-based Feature Extraction

In this phase, the image is converted into a mathematical form using the Grassmann manifold approach. The algorithm used in this approach extracts the essential geometric features of the users, which are then converted into a subspace form. The feature vector extracted in this phase is securely stored as the user's biometric image in the database. The feature subspace is defined as $G(k, n)$

k = subspace dimension

n = feature space dimension

Similarity between stored template S and input template T is computed as:

$$\text{Sim}(S, T) = \|S^T T\|$$

If:

$$\text{Sim}(S, T) \geq \theta$$

(where θ is threshold), authentication is successful.

Where,

D. User Authentication and Similarity Matching

During the process of user authentication, a live face image is captured using the same preprocessing and

the feature extraction techniques are before. The extracted features are compared to the stored template using a similarity measurement technique. A similarity score is calculated, and if it is greater than the threshold value, the user is authenticated. If not, it is an unauthorized attempt and is passed to the intrusion detection module.

Authentication Output:

$$A=1, \text{Sim} \geq \theta$$

$$A=0, \text{Sim} < \theta$$

If $A=1$, access granted.

If $A=0$, intrusion detected triggered.

E. Authorization and Access Control

After the successful authentication, the authorization module allows controlled access to the cloud resources. User specific permissions are implemented to allow users to access only their own files. This phase of authorization acts as a security gateway to the cloud file operations after the identity verification of the users. The access control activities are recorded in the audit logs.

F. Secure File Upload And AES Encryption

After the user is authorized, he or she can upload a file to the cloud platform. However, before the file is stored in the cloud, it is encrypted using the AES encryption technique. The file is divided into blocks, and the encryption process is repeated a number of times using a secret key. The data is converted into a different form to ensure that it remains safe.

Let:

Plaintext file = P AES key = K

First Encryption:

$$C = \text{AES}(K, P)$$

Key Encryption using ECC:

$$K' = \text{ECC}(\text{Public Key}, K)$$

This ensures dual-layer security where the file is encrypted using AES and the encryption key is secured using ECC.

G. Encrypted Cloud Storage And Retrieval

The encrypted file is sent to the cloud storage server, where it is stored in encrypted format. Only the encrypted version of the file is stored on the server to avoid leakage of the data. When the user wants to retrieve the file, his/her identity is verified again, and the file is decrypted using the appropriate AES

key. The original file is sent to the user who has been verified.

H. Intrusion Detection And Alert Mechanism

In case of failure of the authentication process, the intrusion detection module will be activated by the system. The details of the failed attempt, the facial image, the time of the attempt, etc., will be noted in the security log files. If multiple suspicious attempts are detected, the system will analyze the attempt to detect the threat. An alert message will be sent to the administrator, and access will be denied immediately.

V. RESULTS AND DISCUSSION

The Adaptive Secure File System was implemented to test the accuracy of the authentication process, the efficiency of the encryption process, the effectiveness of the intrusion detection system, and the system resources used. The system was tested in different scenarios to evaluate the performance and reliability of the system.

A. Authentication Performance

The Grassmann manifold-based facial biometric authentication module was tested using different registered users in different lighting conditions and facial expressions. The system exhibited high accuracy in the authentication process, yielding a high True Acceptance Rate (TAR) and low False Acceptance Rate (FAR). The similarity threshold was carefully tuned to achieve high accuracy in the authentication process. The results show that the Grassmann manifold approach can handle minor variations in the orientation and lighting conditions, resulting in a lower false rejection rate and a high resistance to false acceptance.

B. Encryption Performance

The double AES encryption process was tested based on encryption time, decryption time, and throughput according to different file sizes. From the experimental results, it was found that encryption time increases proportionally with the size of files. Even though two layers of encryption increase computational overhead by applying single AES algorithm, it still performs within acceptable limits. It ensures efficient throughput and does not delay file upload and retrieval processes.

The performance of the encryption algorithm was tested with AES file encryption and ECC-based key protection with varying file sizes. From the result, it is evident that AES offers efficient file encryption with low computational overhead. Thus, it is suitable for cloud storage. Encryption time is proportional to file size, which does not affect system performance. ECC offers strong security with key protection using smaller key size and low complexity. Thus, it is suitable for cloud storage. AES with ECC offers dual-layer security, ensuring data confidentiality and key protection. Even if encrypted data is accessed, without the key, data is not exposed. Thus, it offers strong and reliable cloud data security.

C. Intrusion Detection Evaluation

The performance of the intrusion detection module was evaluated using a simulation in which several attempts to breach the system were made, and the accuracy and the speed of the system's reaction were determined. During the simulation, the system was able to identify the several attempts to breach the system using a facial recognition system and label them as potential security breaches.

The system was also effective in logging each breach attempt as well as the relevant details such as the time and the system number of attempts made. The system was also effective in its quick response to breach attempts. Once the system identified that the person attempting to get into the system had failed to authenticate themselves using the facial recognition system, the system immediately generated alerts to the effect.

Thus the intrusion detection module was effective in the following ways: it enhanced the System's ability to respond to security breaches in the system as well as in the cloud environment.

D. Resource Analysis

In this section resource utilization is discussed in terms of CPU utilization, storage overhead, and the system latency. The facial image preprocessing and Grassmann feature Extraction required moderate CPU utilization during the authentication process. The use of double encryption based on AES does not show any severe degradation in system performance. Memory utilization is constant due to efficient storage of templates and handling of encryption files. Storage overhead is also moderate

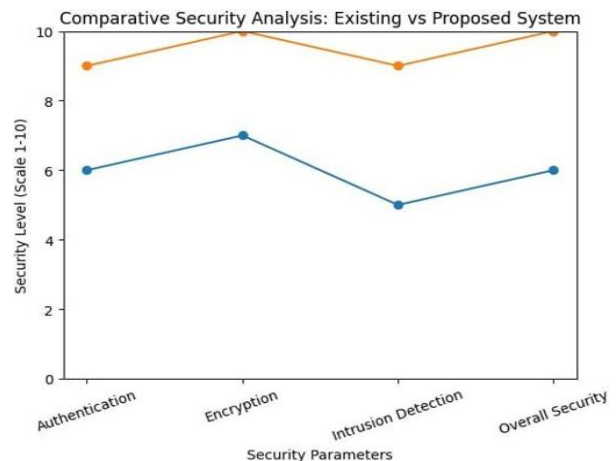
since only encrypted file and small biometric template were stored.

E. Comparative Analysis

The proposed Adaptive Secure File System is compared with traditional cloud storage system based on security parameters like authentication strength, encryption depth, intrusion detection and security integration.

The traditional systems mostly used password authentication and a simple encryption scheme. These systems are easily susceptible to threats like phishing, brute-force, and key compromise. On the other hand, the proposed Adaptive Secure File System has implemented a Grassmann-based facial authentication, AES encryption with ECC-based key protection and intrusion detection in a unified way.

The comparison has proved that the proposed Adaptive Secure File System has better authentication, data confidentiality, and monitoring along with better security and resilience against cyber threats.



F. Discussion

The comparative analysis indicates that the proposed Adaptive Secure File System provides better security for the cloud than other traditional security measures. The use of Grassmann-based facial authentication provides better security for user identities and minimizes the risks that might be present in password authentication system. The use of AES encryption combined with ECC based key protection provides enhanced data and key security of data, as it provides a secondary security layer, which

ensures that data remains secure even in case of a key breach. The intrusion detection feature provides better security for the cloud.

VI. CONCLUSION

In this paper, a secure cloud storage system that utilizes advanced biometric authentication and a dual-layer encryption mechanism was proposed. The proposed system, which utilizes a combination of Grassman manifold-based facial recognition and cryptographic techniques, can address the security of a conventional cloud computing environment. This is because only authorized users can access the information, thereby making the system more reliable and trustworthy.

The proposed Grassman manifold-based facial recognition technique provides a more robust and accurate solution compared to conventional facial recognition techniques. This is because the proposed technique can effectively recognize the facial features, thereby reducing the false acceptance and rejection rates. This makes the proposed facial recognition technique more secure.

In addition to this, the system also uses AES encryption to secure the data of the users before it is stored in the cloud. This is because AES provides high-speed and secure encryption of data, which is necessary to handle a large amount of data. Moreover, the encryption of the AES key using ECC adds an extra layer of security to the system, thereby preventing it from possible attacks and unauthorized access.

The inclusion of the intrusion detection module in the system adds greater security to it. This is because, in the event of failed authentication, the image of the intruder is captured and alerts are sent to the data owner in real time using email. This not only responds to them in a timely manner.

Overall, the proposed system represents a holistic and effective solution of the management of cloud data in a secure manner. The system is able to overcome the shortcomings of the existing systems by incorporating the benefits of biometric authentication, data encryption, and real-time monitoring. The system is also expandable to incorporate the latest technologies, thereby representing a future-proof solution for cloud data security.

REFERENCES

- [1] K. Sasikumar and S. Nagarajan, "Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 392–402, 2025, DOI: 10.1109/OJCS.2025.3538557.
- [2] D. Wu, L. Li, W. Tian, H. Xian, and C. Tian, "Biometric identification on the cloud: A more secure and faster construction," *Information Sciences*, vol. 669, May 2024, DOI: 10.1016/j.ins.2024.120553.
- [3] N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," *Sensors*, vol. 25, no. 1, Jan. 2025, DOI: 10.3390/s25010079.
- [4] S. Shabnam Nasim, P. Pranav, and S. Dutta, "A systematic literature review on intrusion detection techniques in cloud computing," *Discover Computing*, vol. 28, article 107, 2025, DOI: 10.1007/s10791-025-09641-y.
- [5] M. Carvalho, F. Sá, and J. Bernardino, "Evaluation of the Impact of AES Encryption on Query Read Performance Across Oracle, MySQL, and SQL Server Databases," *Cryptography*, vol. 9, no. 4, 2025, DOI: 10.3390/cryptography9040077.
- [6] D. Palma and P. L. Montessoro, "A Post-Quantum Cryptography Enabled Feature-Level Fusion Framework for Privacy-Preserving Multimodal Biometric Recognition," *Cryptography*, vol. 9, no. 4, 2025, DOI: 10.3390/cryptography9040072.
- [7] R. Dash, P. Sarma, and D. Samanta, "Privacy preserving unique identity generation from multimodal biometric data for privacy and security applications," *Security and Privacy*, vol. 7, no. 3, 2024, DOI: 10.1002/spy2.375.
- [8] S. Vatchala, C. Yogesh et al., "Multimodal Biometric Authentication: Leveraging shared layer architectures for enhanced security," *IEEE Access*, vol. 13, 2025, DOI: 10.1109/ACCESS.2025.3534223.
- [9] H. Kim, "Security Enhancement of biometric-based authentication systems using smart card," *IEEE Access*, vol. 12, 2024, DOI:

- 10.1109/ACCESS.2024.3502632.
- [10] A. Odeh, E. Abdelfattah, and W. Salameh, "Privacy-preserving data sharing in telehealth services," *Applied Sciences*, vol. 14, no. 23, 2024, DOI: 10.3390/app142310808.
 - [11] B. D. Deebak and S. O. Hwang, "Privacy preserving seamless authentication with provable key verification using mIoMT for B5G-enabled healthcare systems," *IEEE Transactions on Services Computing*, vol. 17, no. 3, 2024, DOI: 10.1109/TSC.2024.3382950.
 - [12] S. Guo, H. Mu, X. Liu, and H. Ren, "Federated learning for biometric recognition: a survey," *Artificial Intelligence Review*, vol. 57, 2024, DOI: 10.1007/s10462-024-10847-7.
 - [13] A. Mohammed, A. Salama, N. Shebka, and A. Ismail, "Enhancing Network Access Control using Multi-Modal Biometric Authentication Framework," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 1, 2025, DOI: 10.48084/etasr.9554.
 - [14] "A proposed biometric authentication hybrid approach using iris recognition for improving cloud security," *Heliyon*, 2024, DOI: 10.1016/j.heliyon. 2024.e3
 - [15] Kumar, Kukatlapalli Pradeep, et al. "Secure approach to sharing digitized medical data in a cloud environment." *Data Science and Management* 7.2, (2024), DOI: 10.1016/j.dsm.2023.12.001