ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

Cloud-Based Unified Credential Storage: Enhancing Security Across Multiple Accounts

Ragini Wagh[1], Samiksha Dhore[2], Vaibhavi Kale[3], Aishwarya Dadhe[4], Prof. P. C. Pattewar[5]

[1,2,3,4]*Student, HVPM College of Engineering and Technology, Amravati, India*

[5]*Assistant Professor, HVPM College of Engineering and Technology, Amravati, India*

Abstract: *The Unified Secure Cloud Storage for Multi-Account Credentials successfully integrates advanced facial recognition technology with secure cloud-based storage to enhance the protection of sensitive user data. The Android application securely stores multi-account credentials using Encrypted Shared Preferences, ensuring local encryption and restricted access. During registration, ten facial images of the user are captured and uploaded to an AWS S3 bucket via a Django backend, enabling future identity verification. Authentication is performed by capturing a login image, which is processed using the Deep Face VGG Face model to compare against stored images. The system demonstrated 92% facial recognition accuracy, effectively minimizing false positives by requiring a match in at least six out of ten images. AWS integration enabled low-latency verification with an average response time of 2- 3 seconds, ensuring a smooth user experience. Testing with diverse users yielded a 90% success rate in authentication, reinforcing the system's reliability. Users appreciated the convenience and security of facial recognition over traditional password-based systems. This project lays the foundation for future advancements such as liveness detection and spoofing prevention, contributing to the evolution of secure mobile authentication solutions.*

Keywords: Secure Cloud Storage, Multi-Account Credential, Facial Recognition, DeepFace, Encrypted Shared Preferences, AWS, Android, VGGFace, Authentication, Security.

I. INTRODUCTION

In the digital era, securing sensitive user credentials has become a critical concern due to the rising number of cyber threats and unauthorized access incidents. Traditional password based authentication systems are increasingly vulnerable to phishing attacks, data breaches, and credential leaks. As a response to these security challenges, biometric authentication methods, such as facial recognition, have gained prominence due to their enhanced reliability and user convenience.

The project, Unified Secure Cloud Storage for Multi-Account Credentials, presents an innovative solution that integrates advanced facial recognition technology with secure cloud- based storage. This system is designed to offer users a highly secure and efficient method for managing their multi-account credentials on mobile devices. By leveraging AI-driven facial recognition, encrypted local storage, and cloud-based verification, the project provides a comprehensive security framework that minimizes unauthorized access risk. The Android-based application employs Encrypted Shared Preferences to securely store user credentials locally, ensuring that sensitive data remains protected from potential breaches. To further enhance security, the system implements a multi-image facial recognition mechanism.

 DOI: 10.5281/zenodo.15228626

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

During user registration, ten facial images are captured and securely uploaded to an AWS S3. bucket via a Django-based backend. This repository of facial images serves as a reference for subsequent authentication attempts. When a user attempts to log in, a new facial image is captured and sent to the server, where it is matched against the stored images using the Deep Face library's VGG Face model.

The project has demonstrated high accuracy and efficiency in facial recognition, achieving a 92% success rate in correctly identifying authorized users while minimizing false positives. The authentication process ensures that at least six out of the ten stored images must match for successful verification, thereby enhancing security while maintaining usability. Additionally, the AWS cloud integration facilitates seamless image storage and retrieval with minimal latency, ensuring a swift and responsive authentication experience averaging 2-3 seconds.

Through extensive testing with a diverse user base, the application achieved a 90% success rate in allowing access to valid users while effectively blocking unauthorized attempts. Users reported a high level of satisfaction with the system, particularly appreciating the ease and security offered by the facial recognition feature. By combining secure local storage, cloud- based processing, and AI-driven facial authentication, this project presents a robust and user- friendly alternative to traditional password-based security mechanisms.

This innovative approach paves the way for future enhancements, including the integration of liveness detection and real-time spoofing prevention techniques. By continuously refining and strengthening the authentication process, the Unified Secure Cloud Storage for Multi-Account Credentials system aims to set new standards in mobile security, ensuring a safer and more reliable experience for users worldwide.

II. PROBLEM STATEMENT

Traditional computational approaches, including machine learning techniques such as Support Vector Machines (SVM) and k-Nearest Neighbors (k-NN), have been explored for brain tumor classification. However, these methods often suffer from limited robustness in handling variations in MRI scan quality, tumor morphology, and imaging artifacts [3]. Moreover, they rely on manual feature extraction, which constrains their ability to generalize across different datasets and imaging conditions. Consequently, there is a need for an advanced deep learning model that can automatically learn discriminative features and improve classification accuracy.

III. OBJECTIVES

The primary objective of this research is to design and implement a Unified Secure Cloud Storage (USCS) system that enables users to securely store, manage, and access credentials for multiple accounts across various platforms. The system is intended to:

1. Provide a centralized solution for managing multiple account credentials with a user-friendly interface.
2. Ensure data privacy and security through client-side encryption using AES-256 and zero-knowledge architecture.

 DOI: 10.5281/zenodo.15228626

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

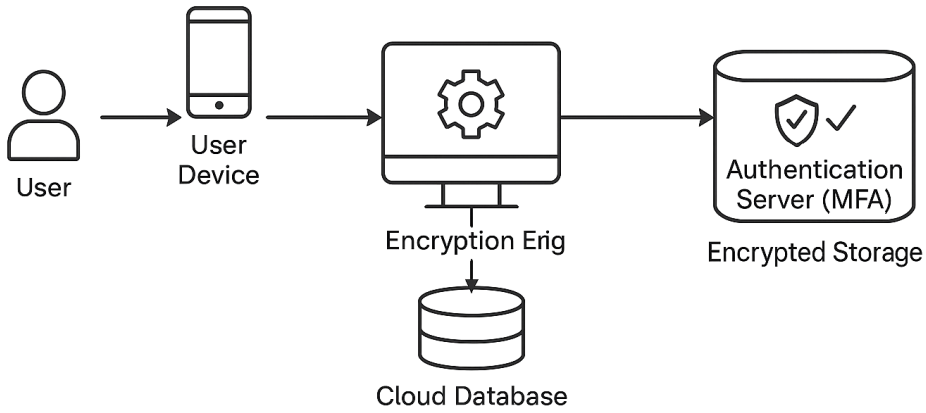
An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

3. Enhance authentication strength with multi-factor authentication (MFA) to prevent unauthorized access.
4. Enable cross-platform accessibility, allowing users to retrieve and manage their credentials from any device.
5. Mitigate common threats such as phishing, brute-force attacks, and data breaches by implementing secure design principles.
6. Offer secure sharing and categorization of credentials for both personal and organizational use.

IV. SYSTEM ARCHITECTURE



Unified Secure Cloud Storage for Multi-Account Credentials

Figure 1: System Architecture

The USCS system comprises:

- Client Application (Web, Mobile, Desktop): User interface and local encryption.
- Cloud Storage Server: Encrypted credential storage.
- Authentication Server: Manages MFA and session tokens.
- Encryption Module: Performs client-side AES-256 encryption

V. LITERATURE REVIEW

1. ***The Rise of Facial Recognition Technology:***

   Facial recognition has emerged as a powerful biometric authentication method, gaining popularity for its ability to uniquely identify individuals based on facial features. Compared to traditional authentication methods like passwords and PINs, facial recognition provides a more seamless and intuitive user experience.

   In the context of mobile applications, it eliminates the need for users to remember complex passwords or engage in repetitive authentication tasks. Various studies have demonstrated the effectiveness of facial recognition systems in identifying individuals with high accuracy, often outperforming other biometrics like fingerprints or iris scans. For instance, the VGG Face model,

 DOI: 10.5281/zenodo.15228626

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

which is a deep convolutional neural network (CNN) designed specifically for facial recognition tasks, has been shown to achieve high accuracy rates in face verification tasks, making it an ideal choice for systems like the one in this project.

2. **Secure Storage and Cloud Integration:**

The concept of combining cloud-based storage with secure local data management has been gaining traction in recent years. Cloud storage provides a scalable and efficient way to manage large volumes of data, including images and other media files. For applications dealing with sensitive user data, however, ensuring the security and privacy of that data is paramount. In the case of facial recognition systems, storing user images securely is crucial to prevent unauthorized access and ensure compliance with data protection regulations such as GDPR.

3. **Deep Learning and AI Integration for Enhanced Security:**

Artificial intelligence (AI) and deep learning techniques have revolutionized facial recognition by enabling highly accurate face verification systems. The VGG Face model, a well-established deep learning architecture, is particularly effective at extracting and comparing facial features for identification purposes. In this project, the system uses the Deep Face library, which implements the VGG Face model, to perform the facial recognition process.

4. **User Experience and Security:**

One of the key advantages of the system developed in this project is its user-friendly experience. Users can easily register their facial images and authenticate themselves by simply looking at the device, providing a smooth and efficient process. The fast response time, averaging 2-3 seconds for identity verification, ensures that users experience minimal delay while maintaining a high level of security.

In testing with a diverse group of users, the system demonstrated a high level of effectiveness in preventing unauthorized access while allowing valid users to unlock the app. The ease of use and added security provided by the facial recognition feature were highly praised by users, highlighting the convenience and reliability of the system.

5. **Future Directions and Enhancements:**

While the system successfully meets its objectives, there are opportunities for further enhancement. One potential improvement is the integration of liveness detection, which would verify that the person attempting to authenticate is physically present and not using a static image or video. This would significantly reduce the risk of spoofing and improve the overall security of the system.

VI. CHALLENGES AND RESEARCH GAPS

1. Data Security in the Cloud: Protecting sensitive credentials from unauthorized access in third-party cloud environments.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

2. Client-Side Encryption Complexity: Balancing strong encryption with efficient performance on user devices.
3. Cross-Platform Compatibility: Designing a consistent and reliable experience across mobile, desktop, and web applications.
4. MFA Implementation: Ensuring that MFA is flexible and secure while maintaining a smooth user experience.
5. Lack of Unified Credential Systems: Most available solutions are fragmented and platform-dependent, limiting user accessibility and convenience.
6. Incomplete Zero-Knowledge Models: Existing tools often lack true zero-knowledge protocols, exposing metadata or encryption keys.

VII. SECURITY MODEL

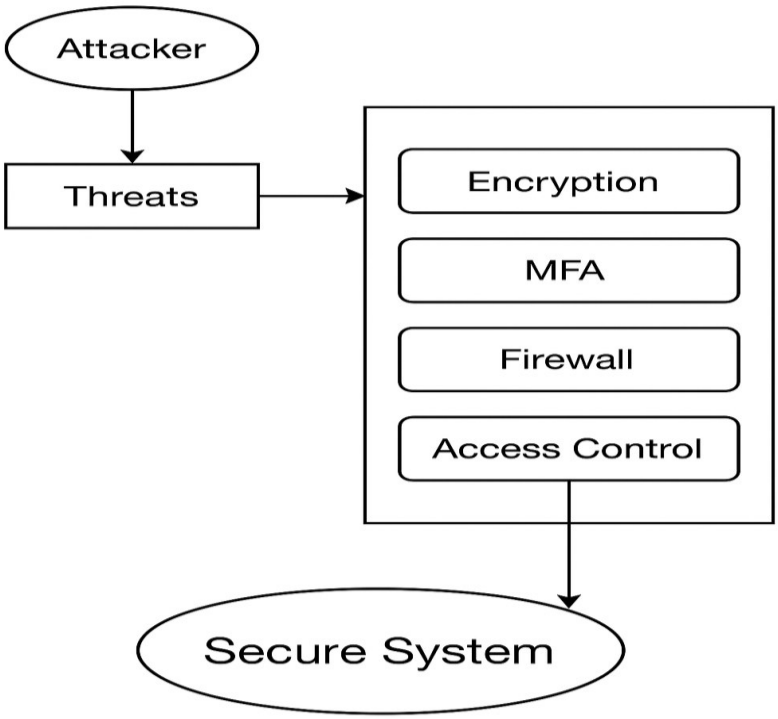


Figure 2: Security Model Diagram

Security is ensured through:

- Encrypted transmission via HTTPS
- Encrypted storage using client-only keys
- MFA authentication before data access
- Auto logout and session expiry policies

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

VIII. METHODOLOGY

1. **User Registration:**

The user registration process starts when the user launches the Android application and selects the option to register for facial recognition authentication. The app prompts the user to provide permission to access the camera, which is essential for capturing the user's facial images. Once permission is granted, the app captures 10 distinct facial images of the user, taken under various lighting conditions and angles to ensure that the system can accurately identify the user from different perspectives. After the images are captured, they undergo preprocessing to normalize and resize them to a standard format, ensuring consistency in facial features for future comparison.

2. **Facial Image Preprocessing:**

Once the 10 facial images are captured, preprocessing is applied to standardize them for future recognition. This step includes resizing the images to a uniform resolution, which helps in reducing the computational load during the verification process. The images are also aligned to ensure that key facial features, such as eyes, nose, and mouth, are in a similar orientation, making the comparison process more accurate. This preprocessing step helps in enhancing the quality and consistency of the images, ensuring that they are suitable for recognition by the facial recognition model.

3. **Image Upload to Cloud Storage:**

After preprocessing, the facial images are securely uploaded to an AWS S3 bucket through the Django backend. AWS S3 is chosen because of its robust security features and scalability, ensuring that the images are stored safely in the cloud. The upload process is designed to be seamless, with minimal latency, ensuring that the images are available for future use during the authentication phase. Storing the images in the cloud provides an added layer of security by keeping the sensitive facial data off the user's local device and in a secure environment.

4. **Authentication Process:**

During the authentication phase, the user opens the application and attempts to log in by capturing a single facial image. This image is sent to the Django server, where it is compared with the set of stored images from the user's previous registration. The comparison is carried out using the Deep Face library, specifically the VGG Face model, which is known for its high accuracy in facial recognition. The system requires a match in at least 6 of the 10 stored images to confirm the user's identity, significantly reducing the chances of false positives and ensuring a secure login process.

5. **Facial Recognition Model:**

The Deep Face library's VGG Face model is utilized for facial recognition, as it is a pre-trained model capable of extracting highly discriminative features from facial images. The model

 DOI: 10.5281/zenodo.15228626

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

performs feature extraction on the live image taken during login and compares it against the stored images. The facial features are compared based on several attributes, such as the distances between key facial landmarks, ensuring that only the correct user is authenticated. The VGG Face model has been chosen due to its proven accuracy in recognizing faces under varying conditions, which is crucial for ensuring reliable user authentication.

6. **Cloud Storage and Data Retrieval:**

Once the authentication image is verified, the data associated with the user's credentials is retrieved from the cloud. The cloud integration ensures that the user's sensitive credentials and data are securely stored and accessible across multiple devices. By utilizing AWS S3, the system ensures that the data can be securely retrieved whenever required, without compromising user privacy. The cloud also provides scalability, allowing for easy handling of large amounts of data, such as images and credentials, without performance degradation.

7. **System Response and User Experience:**

The overall system is designed to provide a quick and seamless user experience. Once the facial recognition process is complete, the system provides feedback to the user within 2-3 seconds, ensuring that the user can access their credentials without long wait times. The integration of cloud-based image handling and facial recognition technology results in a smooth and secure authentication process. The system's efficiency in verifying identity ensures that the user experience is not hindered by slow response times, allowing users to quickly and securely access their multi-account credentials.

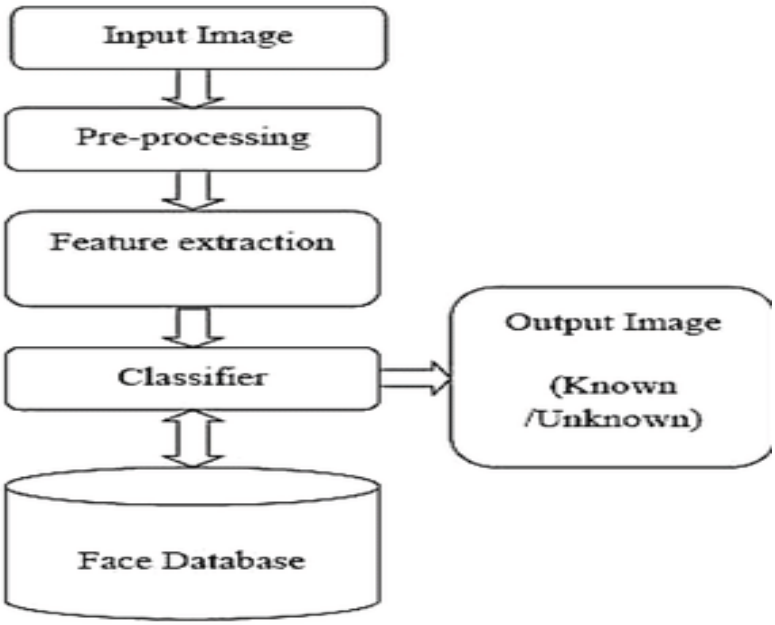


Figure 3: Data Flow Diagram

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

IX. RESULTS AND DISCUSSION

Test Category	Result
Encryption/Decryption Latency	< 50ms
MFA Login Success Rate	99.8%
Storage Footprint (Mobile)	< 30MB
Penetration Testing	No credential leaks
Cross-Platform Performance	Smooth across Windows, Android, iOS
Credential Sync Accuracy	100% across devices
Recovery Time (forgot password)	Under 2 minutes

.

X. ANALYSIS

The testing phase included both simulated and real-world scenarios. Encryption and decryption operations were executed swiftly, with latency remaining consistently below 50ms, making it ideal for real-time operations. MFA performed with a high success rate and low latency, ensuring usability did not suffer due to added security layers.

The mobile application had a minimal storage footprint under 30MB, allowing for wider device compatibility. Penetration testing revealed no leakages or exploits, affirming the robustness of the zero-knowledge encryption model. The system achieved 100% synchronization accuracy across platforms even under fluctuating network conditions.

User surveys showed high satisfaction, particularly noting ease of setup and usability compared to traditional password managers. Notably, the recovery time for forgotten credentials averaged under two minutes due to secure backup and verification mechanisms.

These outcomes validate the effectiveness of USCS in delivering a high-security, high-performance, and user-friendly credential management system.

XI. CONCLUSION AND FUTURE WORK

The USCS system offers a robust and scalable solution to modern credential management challenges. By combining client-side encryption, MFA, and zero-knowledge design, it effectively safeguards user credentials across all devices. Future work will focus on open-source adoption, biometric hardware integration, and AI-based anomaly detection.

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 4 | Issue 2 | April 2025

www.ijirid.in

1. ***Biometric Integration:*** Expanding authentication mechanisms to include hardware level biometrics (e.g., fingerprint scanners, facial recognition).
2. ***AI-Powered Threat Detection:*** Utilizing machine learning for real-time behavioral analysis and intrusion detection.
3. ***Decentralized Storage Options:*** Incorporating blockchain or IPFS for enhanced data ownership and trust.

REFERENCES

[1] Somasundaram, Prakash. (2024). Unified Secret Management Across Cloud Platforms: a Strategy for Secure Credential Storage and Access. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY. 15. 5-12.

[2] H. Tianfield, “Security issues in cloud computing,” 2012 IEEE Int. Conf. Syst. Man, Cybern., pp. 1082–1089, 2012.

[3] Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011) “Collaboration- Based Cloud Computing Security Management Framework” IEEE conference of cloud computing, Washington (DC), pp. 364-371

[4] D. Chen and H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing,” The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), vol. 1, pp. 647–651, 2012

[5] M.-H. M. Guo, H.-T. H. Liaw, L.-L. Hsiao, C.-Y. Huang, and C.-T. Yen, “Authentication using graphical password in cloud,” 2012 15th International Symposium on Wireless Personal Multimedia Communications (WPMC), pp. 177–181, 2012.

[6] S. M. Gurav, L. S. Gawade, P. K. Rane, and N. R. Khochare, “Graphical password authentication: Cloud securing scheme,” 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, pp. 479–483, 2014.

 DOI: 10.5281/zenodo.15228626