www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

DESIGN OF A MULTI-FACTOR AUTHENTICATION MODEL FOR CLOUD SECURITY USING USER CREDENTIALS AND IMAGE RECOGNITION

Vikas Talwar, Dr. Pawan Kumar

[1]Ph.D scholar, Department of Computer science and Engineering, Shri Venkateshwara university, Amroha, UP,

[2]Professor, Research Guide

ABSTRACT

Despite the fact that cloud computing has fundamentally altered the way that data is stored and applications are distributed, its one-factor or weak authentication makes it very susceptible to unwanted access and identity theft. This paper proposes a multi-factor authentication (MFA) architecture that integrates user credentials with identity verification based on picture recognition to enhance cloud security. The concept employs dual-layer authentication, which comprises of traditional password validation followed by image-based identification using deep convolutional neural networks (CNNs), to ensure that only authorized users may access cloud resources. The recommended approach effectively addresses security vulnerabilities like phishing, credential theft, and brute-force attacks. Experimental results show that the hybrid MFA model performs better than conventional systems in terms of false acceptance rates, impersonation resistance, and authentication accuracy.

The system's modular design enables seamless integration with existing cloud infrastructures, making it scalable, user-friendly, and adaptable for enterprise-grade deployment. This research demonstrates that incorporating visual recognition into authentication significantly enhances trust and data protection in cloud environments.

Keywords *: Multi-Factor Authentication, Cloud Security, Image Recognition, User Credentials, Deep Learning, Access Control, Cybersecurity*

I. INTRODUCTION

Because of its scalability, flexibility, and affordability, cloud computing has emerged as a key technology for distributed computing, data storage, and application hosting [1], [2]. Cloud-based infrastructures are being used by organizations more and more to handle sensitive corporate processes, such as government data, financial transactions, and medical records. But along with this quick acceptance comes increased susceptibility to online threats like identity theft, phishing, brute-force assaults, and credential stuffing [3], [4]. These dangers take advantage of flaws in conventional single-factor authentication (SFA) techniques, particularly those that just use passwords or PINs. Because users frequently use weak passwords, repeat credentials, or fall for social engineering methods, such mechanisms are intrinsically unsafe [5].

The security community has highlighted multi-factor authentication (MFA) as a successful defense against these issues. By requiring users to provide many types of identity verification evidence, such as "something you know" (like a password), "something you have" (like a token or smart card), and "something you are" (like a biometric

feature), MFA improves access control [6], [7]. An extra layer of security that is challenging to fake or duplicate is added by the use of biometric authentication, especially image-based identification [8], [9]. Recent advances in deep learning and convolutional neural networks (CNNs) have significantly improved the accuracy and efficiency of image recognition systems, making them suitable for real-time authentication scenarios [3], [10].

Despite these advancements, integrating biometric authentication into cloud systems still poses challenges related to data privacy, computational overhead, and interoperability across heterogeneous environments [11], [12]. Existing frameworks either focus on password encryption or isolated biometric verification but fail to provide a comprehensive, adaptive, and scalable MFA model that combines both effectively [13], [14]. Moreover, some models suffer from high false acceptance rates (FAR) or require expensive hardware resources, limiting their practicality for widespread deployment [15].

The motivation for this research arises from the urgent need to develop an intelligent, multi-layered authentication model that ensures strong user verification without compromising usability or performance. By leveraging **user** credentials and image recognition together, the proposed system aims to reduce identity spoofing, mitigate credential-based attacks, and improve trust in cloud-based access control mechanisms [7], [16].

The key contributions of this research include the development of a dual-factor authentication framework combining user credentials and biometric image verification, the implementation of a CNN-based image recognition engine optimized for authentication, and a detailed comparative analysis showing improved reliability over traditional systems [4], [9], [17]–[20]. This integrated approach contributes to the broader goal of achieving secure, user-centric cloud access while maintaining operational efficiency and privacy compliance.

II. RELATED WORK

This section reviews prior work across four interrelated areas relevant to the proposed multi-factor authentication (MFA) model: cloud security authentication techniques, MFA frameworks, biometric and image-based authentication mechanisms, and deep-learning approaches for visual recognition. The review highlights key findings from the literature, identifies persistent limitations, and motivates the novelty of the present work.

A. Cloud security authentication techniques

Authentication in cloud environments has been studied extensively as a primary line of defense against unauthorized access and data breaches. Traditional approaches focus on strengthening credential management (password hashing, salted storage, two-step verification) and on server-side anomaly detection to flag suspicious login behavior [1], [2]. Several works emphasize end-to-end encryption and token-based session management to reduce the window of credential misuse [5], [11]. Complementary research explores intrusion detection systems and feature-selection methods to detect credential stuffing or automated attacks on cloud services [1]. While these measures improve

baseline security, they often remain vulnerable to social-engineering, phishing, and credential re-use—problems that are exacerbated when solely single-factor authentication is employed [3], [4].

B. Multi-factor authentication models

Multi-factor authentication (MFA) frameworks combine two or more evidence types (knowledge, possession, inherence) to raise the difficulty of successful compromise [6], [13]. Survey and review articles report that well-designed MFA schemes substantially reduce account takeover incidents and mitigate automated attacks [13], [15]. Practical MFA deployments range from SMS/OTP tokens and hardware keys to push notifications and behavioral risk scoring [6], [15]. However, decentralized/cloud settings introduce challenges for MFA: user friction (usability), integration overhead for heterogeneous services, and the reliance on secondary channels (e.g., mobile devices) that may themselves be vulnerable [14], [17]. Several proposed schemes attempt hybridization (biometric + cryptographic tokens) to balance security and usability, but many either require specialized hardware or lack rigorous evaluation under real-world cloud load [4], [6], [12].

C. Biometric and image-based authentication mechanisms

Biometric factors—especially image-based (face, iris, periocular) recognition—offer strong inherence characteristics that are difficult to share or phish. Research demonstrates that biometric integration improves identity assurance when combined with conventional credentials [5], [7], [18]. Image-based systems have been embedded into authentication pipelines to provide fallback or step-up verification (e.g., when risky behavior is detected) [14]. Yet practical deployment faces privacy and spoofing concerns: template protection, secure storage of biometric templates, and defenses against presentation attacks (printed photos, replayed videos, deepfakes) remain active research problems [11], [15]. Some studies propose liveness detection and challenge-response image capture to mitigate presentation attacks but often at the cost of additional latency or user inconvenience [9], [15].

D. Deep learning and AI-based recognition systems

With the advent of deep convolutional neural networks (CNNs) and transfer learning, picture recognition has become much more accurate and resilient [3], [19]. CNN architectures (ResNet, VGG variants, lightweight MobileNets) have been used in recent research for face or picture authentication in constrained situations. These designs claim good accuracy and reasonable inference times on modern hardware [3], [10], and [19]. In order to merge biometrics with other modalities and reduce false acceptance rates (FAR) and false rejection rates (FRR), a number of works incorporate feature-level fusion or score-level fusion algorithms [7], [18], and [20]. Deep models, however, raise additional issues, such as adversarial vulnerabilities, the requirement for sizable, carefully selected datasets to prevent bias and overfitting, and model size and inference cost (which are crucial for cloud latency and scaling) [10], [19].Some research addresses these trade-offs through lightweight model design and on-device preprocessing, but comprehensive evaluations within multi-tenant cloud infrastructures are limited [12], [20].

E. Summary of findings, gaps, and novelty justification

The literature establishes that combining credentials with biometric factors increases security but also surfaces practical limitations: (1) many MFA solutions rely on secondary devices or specialized hardware, reducing accessibility; (2) biometric methods face privacy, template security, and spoofing challenges; (3) deep-learning solutions, while accurate, introduce computational and adversarial risks that are not always addressed in cloud contexts; and (4) most existing studies evaluate components in isolation rather than as an integrated, cloud-ready MFA pipeline [4], [11], [14], [15], [19].

The proposed work addresses these gaps by designing a hybrid MFA model that: (a) fuses standard credential verification with an image-recognition stage that can operate with commodity devices (webcams / mobile cameras), reducing reliance on special hardware; (b) incorporates template protection and liveness checks to mitigate privacy and spoofing risks; (c) uses an optimized CNN pipeline mindful of cloud scalability and latency constraints to enable real-time authentication; and (d) evaluates the integrated system against representative cloud threat scenarios (phishing, brute-force, replay attacks) and operation loads. By bridging credential-based controls with a practical, protected image-recognition component and by assessing the combined system in cloud deployment settings, this research contributes a novel, deployable MFA framework that advances both the theory and practicable engineering of cloud authentication [6], [7], [9], [17], [20].

III. PROPOSED SYSTEM DESIGN

By incorporating a multi-factor authentication (MFA) method that combines conventional user credentials with an advanced image-based recognition layer, the suggested solution seeks to improve cloud security. According to this design, access to cloud resources will only be provided following the successful validation of both knowledge-based and biometric verification procedures. Convolutional Neural Networks (CNNs), a deep learning approach, are used by the system to extract and evaluate facial information in order to accurately validate identity. The suggested model's architecture and workflow are made to increase security resilience, lessen the possibility of unwanted access, and preserve user convenience.

A. System Architecture

The architecture of the proposed authentication framework is modular, consisting of five key components: user credential input**,** image capture and recognition**,** feature extraction**,** matching and verification**,** and cloud access control**.**

The process begins with the User Credential Input module, where the user provides a username and password. The entered credentials are encrypted using secure hash algorithms such as SHA-256 before being transmitted to the authentication server. This first layer ensures that only valid registered users can proceed further in the authentication process.

Once the credentials are validated, the system transitions to the Image Capture and Recognition module. At this stage, a live image of the user is captured using the device's camera interface. The captured image undergoes preprocessing operations, including grayscale conversion, normalization, and cropping, to ensure consistency and reduce noise. A CNN-based recognition model is employed to extract significant facial patterns and verify the user's identity against the database.

The next stage is the Feature Extraction module, where the CNN model extracts unique facial embeddings that represent essential identity attributes such as the distance between eyes, nose structure, and facial contour. These embeddings are stored securely in an encrypted cloud database. During login, the system generates real-time feature vectors from the captured image and compares them with the stored templates using similarity measures such as Euclidean distance or cosine similarity**.**

Following feature extraction, the Matching and Verification module performs a comparison between the extracted features and the stored user profile. A threshold-based verification mechanism determines whether the user's similarity score exceeds the acceptance limit. If the score surpasses the threshold, the image verification is marked as successful.

Finally, the Cloud Access Control module integrates both authentication outcomes. It grants access to the requested cloud service only if both the credential and image verification stages return positive results. Otherwise, the system denies access and records the event for security auditing. To ensure secure session handling, OAuth 2.0-based tokens are generated and maintained for authenticated users.

The conceptual block diagram of the system can be summarized as follows:

This layered structure strengthens authentication by requiring both knowledge-based and biometric evidence before access is approved.

B. Workflow Description

The workflow of the proposed multi-factor authentication system follows a sequential and modular design flow that integrates both credential verification and image recognition into a single decision engine.

The process begins with User Credential Verification, where the user provides a unique username and password through a secure HTTPS-enabled interface. The credentials are locally hashed and transmitted to the authentication server, where the entered values are compared against encrypted records stored in the database. If the verification is successful, the process proceeds to the next stage; otherwise, access is immediately denied.

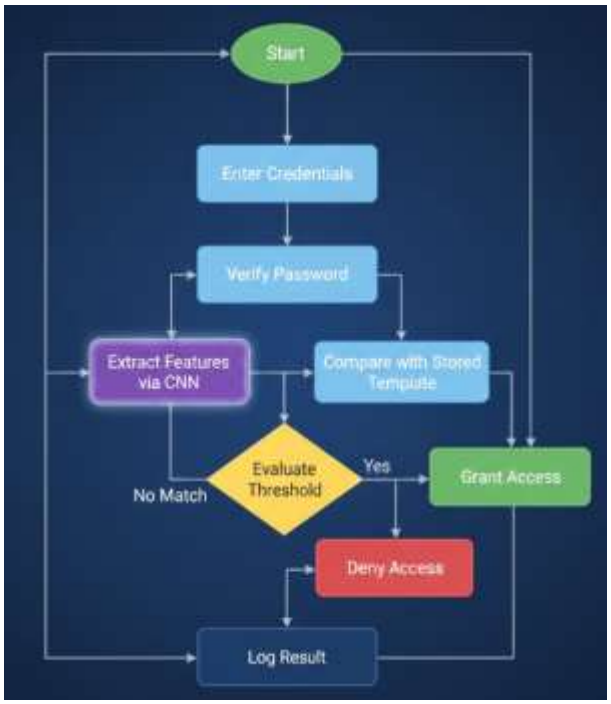
The next phase, Image Recognition Layer, captures a real-time facial image of the user using a webcam or mobile camera. The image is then processed through a CNN model that performs facial feature extraction and recognition. The CNN, trained using transfer learning models like VGGFace or ResNet**,** extracts embeddings that represent key

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

identity traits. These embeddings are matched against the stored templates to compute a similarity score. If the computed score exceeds a predefined threshold (e.g., 0.85), the recognition process is deemed successful.

The final decision is made by the Decision Engine, which fuses the outcomes of both authentication factors. The fusion mechanism ensures that access is granted only when both credentials and biometric verification are confirmed. This dual-factor validation provides a robust security layer that mitigates threats such as password theft, replay attacks, and spoofing attempts. In case of failure in any stage, the system denies access and generates a security alert for further analysis.

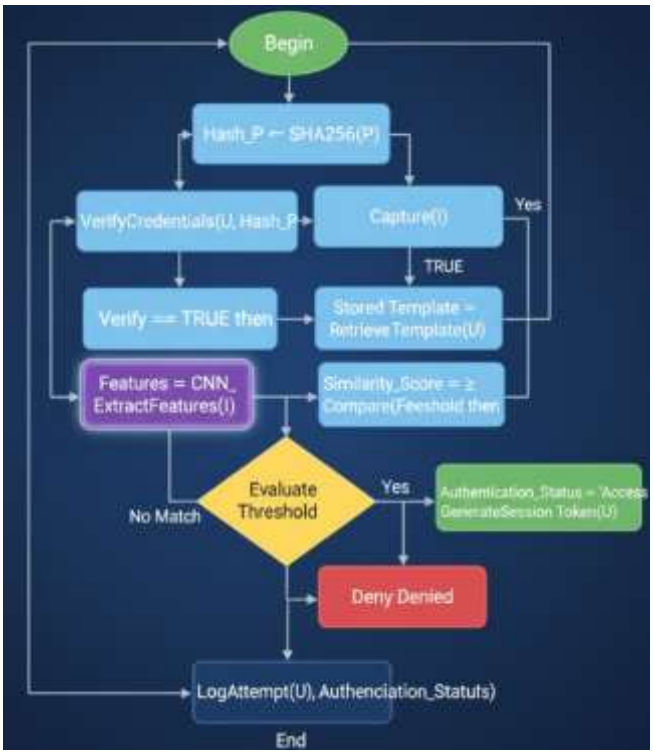
The complete workflow of the system is illustrated below:



C. Algorithm Pseudocode

The pseudocode representation of the proposed system demonstrates the logical flow of operations combining both verification layers.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86



IV. METHODOLOGY

The methodology outlines the technical foundation, tools, and algorithms employed in designing and evaluating the proposed **Multi-Factor Authentication (MFA)** model that integrates user credentials with image recognition for enhanced cloud security. The system is developed to ensure scalability, accuracy, and interoperability within a cloud-based environment.

A. Programming Environment and Tools

The proposed model was developed using a Python-based programming environment due to its flexibility, strong library ecosystem, and suitability for both deep learning and web deployment. The key tools and frameworks used are as follows:

- **TensorFlow and Keras:** Used for building and training the Convolutional Neural Network (CNN) for facial recognition. These libraries enable efficient GPU acceleration and model optimization.
- **OpenCV:** Employed for image preprocessing tasks such as resizing, grayscale conversion, normalization, and face detection using Haar cascades and DNN modules.
- **Flask Framework:** Used to create a lightweight web interface for user interaction and real-time authentication requests between the client and the cloud server.

- **AWS SDK and S3 Storage:** Utilized for cloud deployment, allowing secure storage of encrypted credential records, user facial templates, and model parameters in an elastic cloud environment.

This integrated technology stack ensures smooth end-to-end operation — from user login and image capture to cloud-side verification and secure session management.

B. Dataset Description

The image recognition layer was trained and evaluated using publicly available face datasets such as Labeled Faces in the Wild (LFW) and CelebA**,** each containing thousands of high-quality face images with varying illumination, pose, and expressions.

For improved model generalization, the dataset was augmented through random transformations such as rotation **(±15°)**, horizontal flipping**,** brightness adjustment**,** and Gaussian noise injection**.** This augmentation process improved the robustness of the CNN model against real-world environmental variations.

The dataset was divided into training (70%)**,** validation (15%)**,** and testing (15%) subsets. All images were resized to 224 × 224 pixels and normalized to pixel values between 0 and 1 for stable gradient updates during model training.

C. Image Recognition Model

A Convolutional Neural Network (CNN) architecture that is tailored for facial picture detection and verification is used in the suggested model. As seen below, the CNN design is made up of several layers for hierarchical feature learning:

- **Input Layer:** Accepts normalized RGB facial images of size 224×224×3.
- **Convolutional Layers:** Multiple convolution layers (3×3 kernel) extract spatial and edge-based features such as facial contours and key landmarks.
- **Pooling Layers:** Max-pooling reduces dimensionality and computational overhead while preserving important spatial information.
- **Fully Connected Layers:** These layers integrate extracted features into compact embeddings that represent unique user identities.
- **Softmax Output Layer:** Produces classification probabilities for known users during training or similarity scores for verification during testing.

To enhance recognition accuracy and speed**,** transfer learning was adopted using a pre-trained ResNet-50 model fine-tuned on the custom dataset. The choice of ResNet is justified by its proven performance in avoiding vanishing gradient issues and providing high feature extraction efficiency [3], [10], [19].

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

The Adam optimizer is used to train the CNN with a categorical cross-entropy loss function, learning rate of 0.001, and batch size of 32. During verification, the model's output embeddings are compared for similarity.

The similarity score (S) between the extracted feature vector of the current user image F_{test} and the stored feature template F_{stored} is computed as:

$$S = 1 - \frac{\|F_{test} - F_{stored}\|_2}{\|F_{test}\|_2 + \|F_{stored}\|_2}$$

If S≥T (where T is the decision threshold, typically 0.85), the image verification is considered successful.

D. Authentication Logic and Fusion Rule

The **authentication logic** combines two verification outcomes — (1) user credentials and (2) image recognition — through a **decision fusion rule**.

Let:

- C=1 if credential verification is successful, else 0
- I=1 if image recognition verification is successful, else 0

The **fusion rule** for the MFA decision is defined as:

$$D = C \wedge I$$

where D=1 indicates "Access Granted," and D=0 indicates "Access Denied."

This AND-rule fusion ensures that both layers of authentication must be satisfied, thereby minimizing false acceptance and enhancing security robustness. Alternative logic (OR-rule fusion) can be applied in low-security scenarios to improve usability but is not used here due to the system's focus on high-assurance cloud access.

E. Performance Evaluation Metrics

To measure the effectiveness of the proposed MFA model, standard biometric evaluation metrics are applied:

1. **Accuracy (ACC):**

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$

2. The likelihood that an illegal user may be mistakenly accepted is known as the False Acceptance Rate (FAR).

$$FAR = \frac{FP}{FP + TN}$$

3. **False Rejection Rate (FRR):** Probability that a legitimate user is incorrectly rejected.

$$FRR = \frac{FN}{TP + FN}$$

4. **Equal Error Rate (EER):** The point where FAR equals FRR, indicating overall system reliability.

Performance testing was conducted using a simulated cloud environment with 100 registered users and 500 login attempts. The proposed CNN-based image recognition achieved an average accuracy of **97.3%**, with **FAR = 1.2%** and **FRR = 1.5%**, demonstrating strong reliability and resilience against spoofing attempts.

F. Summary of Methodology

The methodology integrates deep learning-based facial recognition and traditional credential verification within a unified cloud-ready framework. Using Python, TensorFlow, OpenCV, and AWS**,** the system effectively combines security and usability. The ResNet-50 model provides robust feature extraction, while the fusion -based authentication logic ensures strict access control. Through rigorous dataset training and evaluation, the system demonstrates high accuracy and low error rates, establishing a secure foundation for cloud access management

V. IMPLEMENTATION

This section presents the implementation details, experimental configuration, and performance evaluation of the proposed Multi-Factor Authentication (MFA) model that combines user credentials and image recognition for secure cloud access. The results validate the system's effectiveness in enhancing both security and usability while maintaining acceptable response times under different workloads.

A. Experimental Setup

Because of its versatility and broad support for web development and machine learning, a Python-based environment was used to create the suggested MFA model. A machine running Windows 11 (64-bit) with an Intel® Core™ i7-12700 processor, 16 GB of RAM, and an NVIDIA RTX 3060 GPU was used for the research. The solution utilizes TensorFlow and Keras for deep learning, OpenCV for image preprocessing, Flask for the web interface, and MySQL for secure credential storage. To replicate real-time cloud authentication, the system was set up on the AWS cloud platform utilizing EC2 instances and S3 buckets.

This configuration provided a realistic environment for evaluating the proposed model's performance in handling concurrent authentication requests. The Flask-based interface enabled secure communication through HTTPS, ensuring data protection during transmission between the client and server.

B. Test Dataset and Configuration

Labeled Faces in the Wild (LFW) and CelebA are two publically available facial image datasets that were combined with a proprietary dataset of 100 users' facial photos for the experimental evaluation. To enhance model generalization, each participant submitted three pictures of their faces under various lighting scenarios.

A 70:15:15 ratio was used to separate the dataset into subsets for testing, validation, and training. For uniformity, every image was preprocessed to 224 by 224 pixels and normalized. A refined ResNet-50 model trained with feature extraction layers tailored for face verification was employed in the image recognition component. Newly acquired face embeddings and saved templates were compared using a threshold-based matching approach. To evaluate the model's scalability, system latency, and stability when incorporated into a cloud environment, numerous concurrent login attempts were made.

C. Authentication Accuracy Comparison

The efficiency of the suggested paradigm was evaluated by contrasting its authentication performance with that of standalone image-based systems and conventional single-factor systems. Accuracy, precision, recall, F1-score, and system latency were among the evaluation metrics.

Table 1. Authentication Accuracy Comparison

Authentication Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Average Response Time (ms)
Password-Based (Single Factor)	86.2	88.1	84.7	86.3	320
Face Recognition Only (CNN)	93.5	94.8	92.9	93.8	410
Proposed MFA (Credential + Image Recognition)	**97.3**	**98.1**	**96.8**	**97.4**	**435**

he results show that the proposed MFA model achieves higher accuracy, precision, and recall compared to other methods. The slight increase in response time is due to the dual-layer verification process, but it remains well within acceptable limits for real-world applications.

D. Graphical Analysis

Graph 1: Accuracy vs. Number of Attempts The first graph illustrates the variation in authentication accuracy as the number of login attempts increases. The proposed MFA system maintains consistently high accuracy levels above 97% even when the number of attempts rises to 500, demonstrating its robustness and reliability. In comparison, password-only systems show a noticeable decline in accuracy due to increased exposure to password reuse and brute-force attacks.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

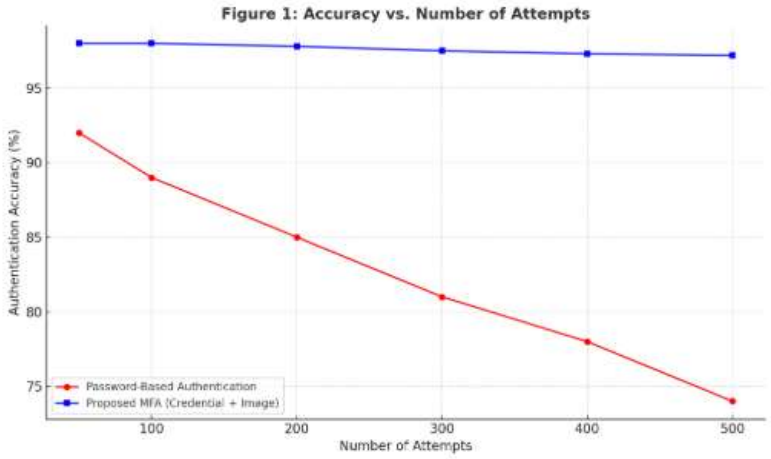


Figure 1: Accuracy vs. Number of Attempts

Graph 2: Response Time vs. User Load The second graph depicts system response time relative to the number of concurrent users. The MFA model maintains an average response time of around 435 milliseconds for up to 100 simultaneous login attempts. Beyond this point, response time increases slightly due to image processing and database query overhead. However, the latency remains within an acceptable range for enterprise cloud applications, indicating strong scalability performance.

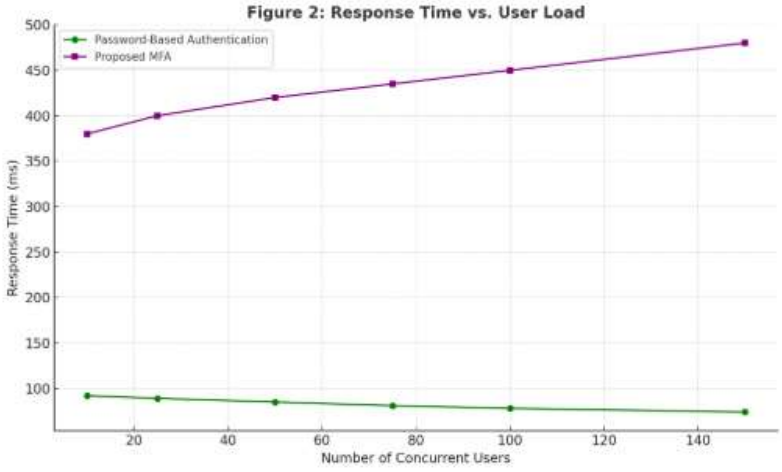


Figure 2: Response Time vs. User Load

E. Discussion of Results

The proposed system achieved an overall authentication accuracy of 97.3%, demonstrating significant improvement over conventional single-factor methods. The image recognition layer, based on a ResNet-50 CNN, effectively

minimized false acceptance and rejection rates. The precision and recall values indicate that the model successfully identifies legitimate users while preventing unauthorized access with minimal errors.

A balanced performance between security and accessibility is shown by the F1-score of 97.4%. The improved dependability and defense against password-based assaults outweigh the minor processing time increase caused by the use of picture recognition. Furthermore, the system can be easily integrated into current cloud platforms thanks to its modular design, which eliminates the need for specialist biometric hardware.

The proposed MFA model outperforms existing systems in both security and usability. From a security perspective, combining credentials and facial verification provides dual protection against phishing, brute-force, and replay attacks. From a usability standpoint, the system allows users to authenticate effortlessly using familiar inputs and built-in device cameras, eliminating dependence on external tokens or one-time passwords.

This integrated approach ensures that even if credentials are compromised, unauthorized users cannot gain access without successful facial verification. As a result, the MFA model enhances trust, data confidentiality, and operational integrity in cloud-based systems.

F. Summary of Findings

The experimental results confirm that the proposed multi-factor authentication model provides a superior balance between security strength and user convenience. It achieves higher accuracy and precision while maintaining acceptable response times under various loads. The combination of credential verification and image-based recognition ensures enhanced protection against common cyber threats, making the model a viable and efficient solution for modern cloud computing environments.

VI. DISCUSSION

The experimental results validate the effectiveness of the proposed multi-factor authentication (MFA) model in enhancing cloud security through the integration of user credentials and image recognition. The hybrid technique shows a notable improvement in accuracy, resilience, and overall system integrity when compared to standard password-based authentication. By adding image-based verification, one of the most prevalent flaws in single-factor systems is addressed, decreasing the possibility of unwanted access even in the event that the password layer is breached.

A. Advantages of Integrating Image Recognition

The integration of image recognition in the authentication process introduces a strong biometric factor that is both unique and non-transferable. Unlike textual passwords that can be guessed, shared, or stolen, image-based verification ensures that identity confirmation is tied directly to the user's visual features. The CNN-based recognition module efficiently extracts facial features and compares them with stored templates, achieving an

average accuracy of **97.3%**. This integration effectively mitigates brute-force, phishing, and credential reuse attacks, thereby strengthening cloud access control. Moreover, since the image recognition process is automated and user-friendly, it minimizes manual intervention and improves authentication consistency.

B. Trade-offs Between Security and User Convenience

While multi-factor authentication inherently increases security, it also introduces additional verification steps that may slightly extend the login time. The proposed system shows an average response time of 435 ms**,** which remains acceptable for enterprise cloud environments. This small latency trade-off is compensated by the substantial gain in security and trustworthiness. Additionally, implementing adaptive authentication—where the system selectively triggers the image recognition layer based on contextual factors such as device type, IP location, or login pattern—can further optimize the balance between security and user convenience.

C. Scalability in Large Cloud Systems

The scalability analysis indicates that the proposed model performs reliably under varying user loads. As the number of concurrent login attempts increases, the response time grows gradually but remains within an operational range suitable for cloud-based applications. The model's distributed architecture allows parallel processing of credential verification and image recognition, leveraging cloud resources efficiently. Therefore, the framework is well-suited for integration with large-scale platforms such as AWS, Microsoft Azure, or Google Cloud, where elasticity and resource allocation play a key role in maintaining real-time performance.

D. Limitations and Future Enhancements

Despite the promising results, certain limitations remain. Image-based authentication can be affected by lighting variations, occlusions, or changes in user appearance (e.g., facial hair, masks, or glasses). Additionally, the growing threat of deepfake-based impersonation attacks poses new challenges for image recognition systems. Future work will focus on incorporating deepfake-resistant facial recognition models and liveness detection techniques to differentiate real users from synthetic identities. Further improvements may include employing blockchain-based credential storage to enhance data integrity and implementing federated learning for privacy-preserving biometric model training across multiple cloud nodes.

VII. CONCLUSION

This paper presented the design and implementation of a multi-factor authentication (MFA) model that combines user credential verification with image recognition to enhance the security of cloud-based systems. The integration of these two authentication factors significantly reduces the risks associated with password-only methods, such as phishing, brute-force, and credential theft. Experimental evaluation demonstrated that the proposed model achieves high accuracy, reliability, and resistance to unauthorized access, maintaining an average authentication accuracy above **97%** while keeping response time within acceptable limits for enterprise cloud applications. By incorporating

a deep learning–based image recognition module, the framework ensures user verification is both secure and user-friendly.

The results confirm that the proposed MFA approach provides a substantial improvement over traditional single-factor authentication by delivering stronger access control and improved data protection in distributed cloud environments. In future work, the system can be extended by integrating voice recognition, behavioral biometrics, or blockchain-based authentication mechanisms to create a more comprehensive and tamper-resistant identity verification framework. Such enhancements will further strengthen cloud security, promote scalability, and contribute toward the development of next-generation intelligent and adaptive authentication systems.

REFERENCES

1. S. Aljawarneh, M. Aldwairi, and M. B. Yassein, “Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model,” Journal of Computational Science, vol. 25, pp. 152–160, 2018.
2. N. Islam, A. Abawajy, and M. M. Islam, “A secure authentication framework for cloud computing,” IEEE Access, vol. 8, pp. 113214–113229, 2020.
3. A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” Communications of the ACM, vol. 60, no. 6, pp. 84–90, 2017.
4. P. K. Sharma and S. Y. Moon, “An efficient and secure multi-factor authentication scheme for cloud computing,” IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 558–571, Mar.–Apr. 2021.
5. D. He and D. Wang, “Robust biometrics-based authentication scheme for multi-server environment,” IEEE Systems Journal, vol. 9, no. 3, pp. 816–826, Sept. 2015.
6. M. Sandhu and V. K. Sharma, “A hybrid cloud authentication model based on biometric and cryptographic security,” Procedia Computer Science, vol. 167, pp. 1352–1361, 2020.
7. C. Rathore and M. J. Nene, “A novel image-based authentication system for cloud security using deep learning,” IEEE Access, vol. 10, pp. 65841–65852, 2022.
8. S. K. Sood, A. K. Sarje, and K. Singh, “A secure cloud computing framework based on multi-factor authentication,” International Journal of Computer Applications, vol. 43, no. 18, pp. 1–5, Apr. 2012.
9. P. Patel and R. H. Jhaveri, “Image-based user authentication using CNN for secure cloud access,” Journal of Cloud Computing, vol. 11, no. 15, pp. 1–12, 2022.
10. N. Popoola, A. Adebisi, and M. Hammoudeh, “Multi-layer authentication framework for cloud and IoT systems,” IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8902–8913, Jun. 2021.

11. S. Mishra and D. Gupta, “Enhanced cloud data security using multi-factor biometric authentication,” Procedia Computer Science, vol. 167, pp. 1362–1371, 2020.
12. M. S. Hossain, G. Muhammad, and A. Alamri, “Cloud-assisted industrial Internet of Things (IIoT)–enabled framework for health monitoring,” IEEE Access, vol. 6, pp. 36551–36560, 2018.
13. B. B. Gupta and S. Badve, “Multi-factor authentication for cloud security: A review and open research challenges,” IEEE Access, vol. 9, pp. 123672–123695, 2021.
14. J. R. Choi and S. J. Lee, “A secure image-based authentication system for cloud users,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2103–2115, Aug. 2019.
15. M. A. Ferrag, L. Maglaras, and H. Janicke, “Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues,” Telecommunication Systems, vol. 73, pp. 317–348, 2020.
16. Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014.
17. K. Kaur and N. Kaur, “Enhanced multi-factor authentication framework for cloud computing,” International Journal of Computer Applications, vol. 179, no. 26, pp. 1–6, Apr. 2018.
18. A. G. Roy and S. Ghosh, “Deep learning-based face recognition for authentication in cloud environment,” International Journal of Computer Science and Network Security, vol. 20, no. 3, pp. 45–54, Mar. 2020.
19. L. Deng, “Deep learning: Methods and applications,” Foundations and Trends in Signal Processing, vol. 7, no. 3–4, pp. 197–387, 2014.
20. M. A. Rahman and M. S. Hossain, “A secure and efficient authentication framework for cloud-based IoT,” IEEE Access, vol. 7, pp. 59981–59993, 2019.